Analytical View of Web Security and Sophisticated Ways to Improve Web Security

Asst. Lect. MSc. IT, Eng. Tamara Saad Mohamed
Baghdad College for economic sciences university, computer science department, Baghdad, Iraq.
Tamara.mohhh@gmail.com

Abstract. All kind of business web application vulnerability statistics are growing in recent and new forms of hacker’s attacks, such as Watering Hole Attack are appearing. Well secured enterprise web applications are threatened by smaller vulnerable webs misused by hackers in targeted attacks. This paper discuss an effective way of creating better secured web application, applicable also in business sector by support them with semantic web platform security and certificate transparency. The main issue – improperly validated user inputs, the biggest security vulnerability often misused by hackers – could be effectively fixed by open-source HTML Purifier library which is usable in various programming languages. Moreover, we will discuss the latest internet security threats and the security of SSL/TSL practice for business web application with proactive on-line embedded prevention, detection and response system.

Keywords: Web application security, internet security threats, Web ecosystem, OWASP, watering hole attack, Dot Net framework, Securing the best SSL/TLS, Content management systems (CMS).

1. Introduction
Using network-based services is an integral part of modern human being. Sensitive information is provided every day to untrusted web applications and therefore not only great web portals are facing the threat of web attacks. In addition, according to the Symantec’s Internet Security Thread Report, the largest growth area for targeted attacks in 2012 (31%) was business. [Ferda Özdemir Sönmez, 2019.] It points to the fact, that small businesses which believed that hacker attacks are targeted especially to larger companies are now very threatened. In addition, overall security level of small business web applications is generally very low in comparison with web portals of great companies. [Bosworth S. Et al, 2009]. Main problem is in insufficient security policy and lack of sophisticated hardware or software Intrusion Detection System (IDS), because in this sector is usually small financial budget for IT security. [Federal Office for information Security (BSI), 2018]. The growing number of web attacks in small business sector is connected with a new type of hackers attack, called Watering Hole Attack. [Hellmann R., 2018.]

2. Web Platform Security
Foundations of the web platform, we briefly describe and discuss the foundations of the Web ecosystem. The goal of this part is to provide the reader with a basic understanding of the Web...
ecosystem, needed to understand the security assessment. Over the last 25 years, the Web ecosystem went through a series of technological waves (As depicted in Figure 1, 2), enriching the platform to the current level where it provides attractive alternative to stand-alone applications (or even replacing the operating system itself). Evolutions in the Web platform include richer presentation capabilities (e.g., graphics, style sheets and multimedia tags), client-side state (cookies and storage), client-side interactivity (JavaScript, the DOM and a rich set of JavaScript APIs), as well as rich Internet Applications (such as Flash, ActiveX and Silverlight).[Ferda Özdemir Sönmez, 2019. & Hellmann R., 2018 & Philippe De Ryck et al. 2014].

3. Microsoft .Net Framework

According to Microsoft ‘.NET is a set of software technologies designed to connect the world of information, people, systems, and devices. The .NET Framework is the ‘programming model that enables developers to build Web-based applications, smart client applications, and XML Web services applications which expose their functionality programmatically over a network using standard protocols such as Simple Object Access Protocol (SOAP) and HTTP[Maskun et al.,2013.]. It is helpful to understand the three basic components of the Framework. These are: The Common Language Runtime, Class Libraries and Assemblies. The .NET Framework provide many useful classes and services that enable developers to easily write secure code and enable system administrators to customize the permissions granted to code so that it can access protected resources. In addition, the runtime and the .NET Framework provide useful classes and services that facilitate the use of cryptography and role-based security. [Varsha R. Mouli et al, 2016. & Hellmann R., 2018. & Aycock J., 2006].

4. EVIDENCE-BASED SECURITY

The .NET Framework determines what permissions should be granted before any code is run. This is known as the code’s evidence. Evidence can be anything and everything that the system knows about the code. Source of evidence includes:[ Varsha R. Mouli et al, 2016. & Hellmann R., 2018. & Federal Office for information Security (BSI). 2018].
1. Cryptography sealed namespaces (strong-named assemblies)
2. Software publisher identity (Authenticode)
3. Code origin (URL, site, Internet Explorer Zone) The permissions that any code will be granted is based on the Security policy.

These permissions can be set by the user or by the administrator. The default security policy installed with the .NET Framework was designed by Microsoft intended for the average user. There are a number of configurable policy levels for the Security policy: [Varsha R.Mouli et al, 2016. & Hellmann R., 2018. & Federal Office for information Security (BSI). 2018]

1. Enterprise Policy ·
2. Machine Policy
3. User Policy
4. Application Domain Policy

5. THE REPORT OF INTERNET SECURITY THREATS IN 2019

Form Jacking: Targeted attacks. Living off the land. Coming for your business. The report analyzes data from Symantec’s Global Intelligence Network, the largest civilian threat intelligence network in the world, which records events from 123 million attack sensors worldwide, blocks 142 million threats daily, and monitors threat activities in more than 157 countries. [Varsha R.Mouli et al, 2016, & S. Joseph, K.P. Jevitha, 2016. & Preeti Sirohi et al, 2016.]

Crypto Jacking: Down, but not out Ran somware and cryptojacking were go-to moneymakers for cyber criminals. But 2018 brought diminishing returns, resulting in lower activity. For the first time since 2013, ransomware declined, down 20 percent overall, but up 12 percent for enterprises. With a 90 percent plunge in the value of cryptocurrencies, cryptojacking fell 52 percent in 2018. Still, cryptojacking remains popular due to a low barrier of entry and minimal overhead; Symantec blocked four times as many cryptojacking attacks in 2018 compared to the previous year. [Varsha R.Mouli et al, 2016, & S. Joseph, K.P. Jevitha, 2016. & Preeti Sirohi et al, 2016.]

Targeted Attacks: Targeted attackers have an appetite for destruction Supply chain and Living-off-the-Land (LotL), attacks are now a cybercrime mainstay: supply chain attacks ballooned by 78 percent in 2018. Living-off-the-land techniques allow attackers to hide inside legitimate processes. For example, the use of malicious PowerShell scripts increased by 1,000 percent last year. Symantec blocks 115,000 malicious PowerShell scripts each month, but this number accounts for less than one percent of overall PowerShell usage. [Varsha R.Mouli et al, 2016, & S. Joseph, K.P. Jevitha, 2016. & Preeti Sirohi et al, 2016.]

Cloud Challenges: If it’s in the cloud, security’s on you A single misconfigured cloud workload or storage instance could cost an organization millions or cause a compliance nightmare. In 2018, more than 70 million records were stolen or leaked from poorly configured S3 buckets. Off-the-shelf tools on the web allow attackers to identify misconfigured cloud resources. Hardware chip vulnerabilities, including Meltdown, Specter, and Foreshadow allow intruders to access companies’ protected memory spaces on cloud services hosted on the same physical server. Successful exploitation provides access to memory locations that are normally forbidden. This is particularly problematic for cloud services because while cloud instances have their own virtual processors, they share pools of memory—meaning that a successful attack on a single physical system could result in data being leaked from several cloud instances. [Varsha R.Mouli et al, 2016, & S. Joseph, K.P. Jevitha, 2016. & Preeti Sirohi et al, 2016.]

Internet of Things (IoT): Your favorite IoT device is an attacker’s best friend Although routers and connected cameras make up 90 percent of infected devices, almost every IoT device is vulnerable, from smart light bulbs to voice assistants. Targeted attack groups increasingly focus on IoT as a soft entry point, where they can destroy or wipe a device, steal credentials and data, and intercept SCADA communication. [Varsha R. Mouli et al, 2016, & S. Joseph, K.P. Jevitha, 2016. & Preeti Sirohi et al, 2016.]

6. Open Web Application Security Project (OWASP) Top Ten Vulnerability of (OWASP)
According to Open Web Application Security Project (OWASP) Top ten Vulnerabilities the most common vulnerability in 2019 is still Injection [Bosworth S. et al, i2009.]. All of the Top ten Vulnerabilities are caused by web application developers, who have not followed the best practices of secure development. Types of attacks which are listed below are in general targeted directly against the web application and it does not even matter how strong firewall rule sets are or how frequent the patching mechanism is as shown in figure 3. The only effective defence is either sophisticated intrusion detection system (IDS), or web built on a secure development framework. [5, 6,7,8,9, 10].

6.1. A1: Injection
Injection happens when an attacker injects a bit of code to trick an application into performing unintended actions. The most common and well-known injection attack is SQL injection (SQL), where an attacker inserts an SQL statement that, for example, exposes the contents of a database table. LDAP injection is a similar type of attack against a directory system. OWASP recommends you check incoming requests to determine their trustworthiness, and keep un trusted data separated from the systems that run your application. [5,6,7,8,9, 10]

6.2. A2: Broken authentication
Formerly “Broken authentication and session management” You know the user credentials of people accessing your systems, but do you know who is actually behind the keyboard? Attackers can hijack user identities and hide behind genuine user IDs to gain easy access to your data and programs. Implement strong authentication and session management controls, and ensure your users are who they say they are. [5,6,7,8,9, 10]

6.3. A3: Sensitive data exposure
Unintended data display is a serious problem to anyone operating a web application that contains user data. Although OWASP points out that the full perils of insecure data extend well beyond the scope of the OWASP Top 10, they do recommend a handful of minimum steps—among them, encrypting all sensitive data at rest and in transit and discarding sensitive data as soon as you can. [5,6,7,8,9, 10]

6.4. A4: XML external entities (XXE)
XML processors are often configured to load the contents of external files specified in an XML document. An attacker can exploit this capability by having the XML processor return contents of local files, access files on other systems that trust the attacked system, or even create executable code. OWASP recommends configuring your XML processor to turn this capability off. [5,6,7,8,9, 10]

6.5. A5: Broken access control
This vulnerability combines the vulnerabilities “Missing function level access control” and “Insecure direct object references” from the 2013 list. Broken access control occurs when users can perform functions above their levels or gain access to other users’ information. OWASP advocates several methods to secure your applications, including establishing “deny by default” rules to allow function access only to users you trust and implementing access control checks for each user-accessible object (such as files, webpages, and other information). [5,6,7,8,9, 10]

6.6. A6: Security misconfiguration
“Security misconfiguration” is a general reference to application security systems that are incomplete or poorly managed. Security misconfiguration can occur at any level and in any part of an application, so it’s both highly common and easily detectable. [5,6,7,8,9, 10]
6.7. A7: Cross-site scripting (XSS)
An XSS vulnerability extends the trust a user has given a specific site to a second, potentially malicious site. Users generally permit trusted sites to perform certain actions. But malicious actors can modify a page on a trusted site to interact with an untrusted site, exposing sensitive data or spreading malware. XSS vulnerabilities are common, but they’re not difficult to remediate. Separate untrusted, user-inputted data from active content in your webpage (for example, hyperlinks). And don’t rely on input validation. [5,6,7,8,9, 10]

6.8. A8: Insecure deserialization
Serialization is used to turn an object into data that can be sent somewhere or stored. In this way, the object can be recreated in the same state by another system and/or at another time via the process of deserialization. An attacker could provide an object that, when deserialized, gives the attacker access privileges or runs malicious code. This vulnerability is difficult to exploit, but it can also be difficult to detect. OWASP recommends restricting the types of objects to be deserialized, or not deserializing untrusted objects at all. [5,6,7,8,9, 10]

6.9. A9: Using components with known vulnerabilities
Open source development practices drive innovation and reduce development costs. But despite the benefits of open source software, the 2018 Open Source Security and Risk Analysis found that significant challenges remain in security and management practices. It’s critical that you gain visibility into and control of the open source components in your applications and Docker containers. [5,6,7,8,9, 10]

6.10. A10: Insufficient logging and monitoring
Sufficient logging and monitoring can’t prevent malicious actors from launching an attack. But without it, you might find it difficult to detect attacks, shut them down, and determine the scope of the damage. Insufficient logging and monitoring is common. But it’s also difficult to detect. Even if your logs are detailed enough to reveal an attack in progress, there’s no guarantee that the systems put in place to monitor those logs are working. [5,6,7,8,9, 10]

7. Watering Hole Attack
In recent year, hackers started to use a new scenario of web attack against enterprise systems. It is type of highly sophisticated targeted attack, which is misusing vulnerable web sites of various entities to defeat the stronger security of another entity. The concept of Watering Hole Attack is similar to a
predator waiting at a watering hole in a desert. The predator assumes, that the prey eventually has to come to refresh and waits for his victim. This hacker’s technique uses vulnerable web sites which are considered to be visited by hacker’s victims. Vulnerable web site is infected by malicious code which is able to install an exploit to victim’s computer. [Ms. V. Revathi, Ramya et al, 2018. & Maskun, et al, 2013.]

8. Problem Solution
The overall security of small business sector web applications should be improved, because this will lead also to higher security level of enterprise sector in the same supply chain. An effective improvement without need of high financial budget could be done using secure open-source frameworks for web application development. By using .NET framework and semantic web supported by Certificate Authority (CA) and SSL/TLS protocol, they are provides more security to web application. By using secure development framework, the developer does not face a large number of issues and places for creating a security bug. The resulting web application should be immune especially to attack, which are based on unvalidated inputs. On the other side, some web application faced logic issues, such as Insecure Direct Object References, can still appear and should be carefully tested within development process. [Yingjie Wang et al, 2019 & Preet Sirohi et al, 2016, Maskun et al, 2013.]

9. Security of the Best SSL/TLS Practices for Business
Symantec is a leading provider of securing more than one million web servers worldwide. When you choose Symantec, you can rest assured that your website and your reputation are protected by the Certificate Authority (CA). [Yingjie Wang et al, 2019 & Preet Sirohi et al, 2016, Maskun et al, 2013.]. By evolving our SSL/TLS certificate standards to the ECC algorithm, we raised our level of security and performance, delivering 64,000 times stronger encryption than the most commonly used SSL certificate. [Yingjie Wang et al, 2019 & Preet Sirohi et al, 2016, Maskun et al, 2013.].

10. Symantec Web and Certificate Transparency
Symantec is pleased to extend support for Certificate Transparency (CT) for our Organization Validation (OV) products, a key certificate management capability for all SSL/TLS certificate types and customer channels. This is just the next step in empowering organizations with the ability to detect and mitigate security concerns for domains they own. By enabling this key certificate management capability, organizations will get a comprehensive view of what active certificates exist for each of their domains. Such transparency lets them effectively manage all active certificates and quickly respond to threats. As shown in table 1.[Ferda Özdemir Sönmeza,2019. & Varsha R. Mouli, 2016.& 9,18].Today, Symantec is one of the few Certificate Authorities to operate its own Certificate Transparency log server and will soon have a second one available. To encourage Certificate Transparency and offer a cost-effective option to the CA ecosystem, Symantec now allows third party Certification Authorities to log their certificates on its servers as well. [Ferda Özdemir Sönmeza, 2019. & Varsha R. Mouli, 2016.& 9,18].While Symantec is strongly advocating for CT, strong certificate management comes in three parts: Prevention, Detection, and Response. [Ferda Özdemir Sönmeza, 2019. & Varsha R. Mouli, 2016.& 9,18].

11. All Symantec SSL/TLS Certificates Come With the Following Prevention
Customers have the ability to specify and control which Certification Authorities are permitted to issue certificates for their domains through the industry-recognized Certification Authority Authorization CAA specification. Symantec introduced support for CAA across all products in mid-
2015 and is championing making this an industry requirement for all Certification Authorities as shown in figure 4. [Yingjie Wang et al, 2019 & Preeti Sirohi et al, 2016. & Maskun et al, 2013.]

Figure 4. Prevention of Symantec SSL/TLS Certificates

12. Detection
Certification Authorities are increasingly recording certificates to public Certificate Transparency log servers which allow customers to monitor what certificates have been issued for their domains. Symantec is extending its support for Certificate Transparency to all of its certificates by default and is championing making this an industry requirement for all Certification Authorities as shown in figure 5 and table 1. [Yingjie Wang et al, 2019. & Preet Sirohi et al, 2016. & Maskun et al, 2013.].

Figure 5. Detection of Symantec SSL/TLS Certificates

| Platform                                      | Extended Validation Certificates | Organization Validation Certificates | Domain Validation Certificates |
|-----------------------------------------------|---------------------------------|-------------------------------------|-------------------------------|
| Symantec Complete Website Security & Managed PKI for SSL | Available                       | Available                           | Not Applicable                |
| Symantec Trust Center                         | Available                       | Available                           | Not Applicable                |
| Thawte Certificate Center                     | Available                       | Available                           | Available                     |
| GeoTrust Security Center                      | Available                       | Available                           | Available                     |
| Rapid SSL                                     | Not Applicable                  | Not Applicable                      | Available                     |
| Symantec Japan SSL                            | Available                       | Available                           | Available                     |

Table 1 Certification Authorities
13. Response

Customers can revoke problem certificates and have that information published immediately through the industry standard Online Certificate Status Protocol (OCSP).

Symantec offers global, high performance OCSP services, processing on average 13 Billion certificate checks every day as shown in figure 6. In Fall-2015, Symantec expanded its OCSP service to include IPv6 support. [Yingjie Wang et al., 2019. & Preet Sirohi et al, 2016. & Maskun et al.,2013.]

![Figure 6 Response of Symantec SSL/TLS Certificate](image)

14. How to Improve the Web Site within Ten Tips

In recent years there has been a proliferation of great tools and services in the web development space. Content management systems (CMS) allow business owners to quickly and efficiently build their online presences. Their highly extensible architectures, rich plugging, module, extension ecosystem have made it easier than ever to get a website up and running without years of learning required. This is undoubtedly a great thing; however, an unfortunate side effect is that now there are many webmasters who do not understand how to make sure their website is secure, or even understand the importance of securing their website. The top 10 steps all webmasters, website owners, can, and should, take to keep their website secure.[Varsha R. Mouli et al 2016.& Aycock J., 2006. & , Bosworth S.,et ali2009. & Hellmann R.,2018.&,10. & Preet Sirohi et al, 2016.& Maskun, Alma Manuputty & S.et al 2013.& 17]

14.1. Update:

Countless websites are compromised every day due to the outdated and insecure software used to run them. It is incredibly important to update your site as soon as a new plug-in or CMS version is available. Most hacking these days is entirely automated, with bots constantly scanning every site they can looking for exploitation opportunities. It is not good enough to update once a month or even once a week because bots are very likely to find a vulnerability before you patch it. Unless you are running a website firewall like Cloud Proxy, you need to update as soon as updates are released.

14.2. PASSWORDS:

Working on client sites, often need to log in to their site/server using their admin user details. We are frequently disturbed by how insecure their root passwords are. It is a little scary that we have to say this, but admin/admin is not a secure username and password combination. If your password appears in this list of most common passwords, it is guaranteed that your site will be hacked at some point. When it comes to choosing a password there are 3 key requirements that should always be followed (CLU – Complex, Long, Unique):

- **COMPLEX:** Passwords should be random.
- **LONG:** Passwords should be 12+ characters long.
- **UNIQUE:** Do not reuse passwords! Every single password you have should be unique.
14.3. ONE SITE = ONE CONTAINER:

We understand the temptation. You have an ‘unlimited’ web hosting plan and figure why not host your numerous sites on a single server. Unfortunately this is one of the worst security practices we commonly see. Hosting many sites in the same location creates a very large attack surface.

For example, a server containing one site might have a single WordPress install with a theme and 10 plug-in that can be potentially targeted by an attacker. If you host 5 sites on a single server now an attacker might have three WordPress installs, two Joomla installs, five themes and 50 plug-in that can be potential targets. To make matters worse, once an attacker has found an exploit on one site, the infection can spread very easily. Not only can this result in all sites being hacked at the same time, it also makes the clean-up process much more time consuming and difficult. The infected sites can continue to re-infect one another in an endless loop.

14.4. SENSIBLE USER ACCESS:

This rule only applies to sites that have multiple logins. It’s important that every user has the appropriate permission they require to do their job; if they require escalated permissions momentarily, grant it, then reduce it once the job is complete. This is a concept known as Least Privileged.

For example, if you have a friend that wants to write a guest blog post for you, make sure their account does not have full administrator privileges. Your friend’s account should only be able to create new posts and edit their own posts because there is no need for them to be able to change website settings. Once you have separate user accounts for every user, you can keep an eye on user behaviour by reviewing logs and knowing the usual behaviour (when and where they normally access the website) so you can spot anomalies and confirm with the person that their account hasn’t been compromised.

14.5. CHANGE THE DEFAULT CMS SETTINGS:

Today’s CMS applications, although easy to use, are horrible from a security perspective for the end users. By far the most common attacks against websites are entirely automated, and many of these attacks rely on the default settings being used. This means that you can avoid a large number of attacks simply by changing the default settings when installing your CMS of choice.

For example some CMS applications are writeable by the user – allowing a user to install whatever extensions they want. There are settings that you may want to adjust to control comments, users, and the visibility of your user information. The file permissions, which we discuss later, are another example of a default setting that can be hardened. It is usually easiest to change these default details when installing the CMS, but they can be changed later.

14.6. EXTENSION SELECTION:

One of the beautiful things about today’s CMS applications is it’s extensibility. What most don’t realize however is that, that same extensibility is it’s biggest weakness. There are a massive number of plugging, add-ons, and extensions providing virtually any functionality you can imagine. However the reality is that at times the massive number of extensions can be a double edged sword. Often there are multiple extensions offering similar functionality, so how do you know which one to install? Here are the things which always look at when deciding which extensions to use. The first thing which looking for is when the extension was last updated. If the last update was more than a year ago then it concerned that the author has stopped work on it. The much prefer to use extensions that are actively being developed because it indicates that the author would at least be willing to implement a fix if any security issues are discovered or reported. Furthermore if an extension is not supported by the author, then it makes little sense to use it for your website as it may stop working at any time. We also like to look at the age of the extension and the number of installs. An extension developed by an established author that has numerous installs is much more trustworthy than one that has 100 installs and has been released by a first-time developer. Not only is the experienced developer much more likely to have a good idea about best security practices, but they are far less likely to damage their reputation by inserting malicious code into their extension. More importantly, the larger the user base, the more incentive attackers have
to invest in trying to break it. It is incredibly important that to download all extensions and themes from legitimate sources.

There are many sites that offer ‘free’ versions that are normally premium and require payment to download. These ‘free’ versions are pirated and frequently infected with malware. The websites offering these ‘free’ versions are setup with only one goal: to infect as many websites as possible with their malware.

14.7. BACKUPS:

Like anything in the digital world, it can all be lost in a catastrophic event. Making backups of website is very important, but storing these backups on the web server is a major security risk. These backups invariably contain unpatched versions of the CMS and extensions which are publicly available, giving hackers easy access to the server.

14.8. SERVER CONFIGURATION FILES:

We should really get to know the web server configuration files. Apache web servers use the .htaccess file, Nginx servers use nginx.conf, and Microsoft IIS servers use web.config. Most often found in the root web directory, these files are very powerful. These files allows you to execute server rules, including directives that improve your website security.

Here are a few rules that recommend the research and add for the particular web server:

- Prevent directory browsing: This prevents malicious users from viewing the contents of every directory on the website. Limiting the information available to attackers is always a useful security precaution.
- Prevent image hot linking: While this isn’t strictly a security improvement, it does prevent other websites from displaying the images hosted on their web server. If people start hotlinking images from specific server, the bandwidth allowance of
- The hosting plan might quickly get eaten up displaying images for someone else’s site.
- Protect sensitive files: Set rules to protect certain files and folders. CMS configuration files are one of the most sensitive files stored on the web server as they contain the database login details in plain text. There may be other locations that can be locked down such as admin areas. Should also restrict PHP execution in directories that hold images or allow uploads.
- There are many more rules and options that can look into for the web server configuration file. Should search for the name of the CMS, web server and “security” but make sure to confirm the findings are legitimate before implementing anything. Some people post bad information online with malicious intent.

14.9. INSTALL SSL:

It has actually of two minds as to whether or not to include this point because there have been so many articles incorrectly stating that installing SSL will solve all security issues. SSL does nothing to protect the site against any malicious attacks, or stop it from distributing malware. SSL encrypts communications between Point A and Point B – the website server and browser. This encryption is important for one specific reason: it prevents anyone from being able to intercept that traffic, known as a Man in the Middle (MITM) attack. SSL is especially important for E-Commerce website security and any website that accepts form submissions with sensitive user data or Personally Identifiable Information (PII). The SSL certificate protects the visitors’ information in transit, which in turn protects the individuals from the fines that come along with being found non-compliant with PCI DSS.

15. File Permissions

File permissions define who can do what to a file. Each file has 3 permissions available and each permission is represented by a number:

- ‘Read’(4): View the file contents.
- ‘Write’(2): Change the file contents.
· ‘Execute’(1): Run the program file or script.
    If the user wants to allow multiple permissions he just need to add the numbers together, e.g. to allow read (4) and write (2) you set the user permission to 6. If you want to allow a user to read (4), write (2) and execute (1) then you set the user permission to 7.

16. There Are Also 3 User Types
· Owner – Usually the creator of the file, but this can be changed. Only one user can be the owner.
· Group – Each file is assigned a group, and any user who is part of that group will get these permissions.
· Public – Everyone else.

So, if the owner want to have read & write access, the group to have only read access, and public to have no access, the file’s permissions settings should be: as shown in table 2

|        | Write | Read | Execute |
|--------|-------|------|---------|
| Owner  | 2     | 4    | 0       |
| Group  | 0     | 4    | 0       |
| Public | 0     | 0    | 0       |

Table 2 file permissions

When view the file permissions this will be shown as 640. Folders also have the same permissions structure, the only difference being that the ‘execute’ flag allows to make the directory your working directory (so usually want it on). [Varsha R. Mouli et al 2016. & Aycock J., 2006. & Bosworth S., Kabay M.E., Whyne E., 2009 & Hellmann R. 2018 & Department for Digital, Culture, 2019. & Preet Sirohi et al 2016. & Maskun, Alma Manuputty, S. et al 2013.7& 17].

17. Conclusion

So from the analytical view we can conclude that the using of semantic web supported by SSL/TLS protocol and CA give more security to the web and business webs, and from the view of sophisticated ways to improve the web security, there are ten relatively simple steps can take to dramatically increase the security of the website. While these steps alone will not guarantee that site is ever hacked, following them will stop the vast majority of automated attacks, reducing overall risk posture. Being aware of these issues and understanding them will provide you with valuable insight into how the underlying technology works and help to make a better web master/site operator.

References
1. Ferda Özdemir Sönmez, 2019. Security Qualitative Metrics for Open Web Application Security Project Compliance, International Symposium on Machine Learning and Big Data Analytics for Cybersecurity and Privacy (MLBDACP) April 29 – May 2, 2019, Leuven, Belgium, ScienceDirect, Procedia Computer Science 151 (2019) 998–1003.
2. Varsha R. Mouli, K. P. Jevitha, 2016. iWeb Services Attacks and Security- A Systematic Literature Review, Procedia Computer Science, Volume 93, 2016, Pages 870-877.
3. S. Joseph, K. P. Jevitha, 2016. Evaluating the Effectiveness of Conventional Fixes for SQL Injection Vulnerability Proceedings of 3rd International Conference on Advanced Computing
Networking and nformatics; (2016), pp. 417-426

[4] Aycock J.,2006.Computer Viruses and Malware”, Springer Science+Business Media LLC, University of Calgary, Canada (2006),ISBN-13: 978-0-387-30236-2.

[5] Bosworth S., Kabay M.E.,Whyne E., i2009.Computer Security Handbook” (5th Edition), John Wiley & Sons, nc., Hoboken, New Jersey (2009),Volume 1., ISBN: 978-0-470-32722-Federal Office for nformation Security (BSI). (2018). “Register of current cyber threats and attacks”, BSI-CS 026, Version 2.0, https://www.allianz-fuer-cybersicherheit.de/

[6] Fuhrberg K.,2000.Internet-Security - Browser, Firewalls and Encryption, Carl Hanser,Verlag, München Wien (2000),ISBN 3-446-21333-3.

[7] Hellmann R.,2018.IT-Security - An ntroduction”, DE Gruyter, Oldenbourg (2018) ISBN 978-3-11-049483-9.

[8] Department for Digital, Culture,2019. Media and Sport Cyber Security Breaches Survey 2019: Statistical Release, Cyber Security Breaches Survey 2019,

[9] Ms. V. Revathi,Ramya ,Gayathri, i2018. iAn Overview: Watering Hole Attack, JSRD - International Journal for Scientific Research & Development. Vol. 6, ssue 01, 2018, SSN (online): 2321-0613.

[10] Yingjie Wang,Xing Liu,Weixuan Mao,We iWang, i2019 i. iDCDroid: automated detection of SSL/TLS certificate verification vulnerabilities n Android apps ,conference paper ,May 2019

[11] Preet iSirohi,Amit Agarwal,Sapna Tyagi, i2016. iA comprehensive study on security attacks on SSL/TLS protocol, Oct 2016,2016 2nd international Conference on Next Generation Computi

[12] Maskun, Alma Manuputty, S. M. Noor,Juajir Sumardi,2013. Cyber Security Rule of Use nternet Safely?:, Procedia - Social and Behavioral Sciences, Volume 103, 26 November 2013, Pages 255-261.

[13] https://www.symantec.com/security-center/threat-report [accessed 30/10/2019].

[14] https://www.giac.org/paper/gsec/2187/microsoft-dotnet-framework-security/103718 [accessed 2/10/2019].

[15] https://www.cgisecurity.com/lib/dotnet-security-framework.pdf [accessed 3/10/2019]

[16] https://blog.sucuri.net/2015/06/10-tips-to-improve-your-website-security.html 10 Tips to improve Your Website Security, [accessed 29/10/2019]

[17] https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-executive-summary-en.pdf, [accessed 28/10/2019]

[18] https://securityboulevard.com/2019/01/owasp-top-10-web-application-security-risks/, OWASP Top 10 web application security risks, [accessed 1/11/2019]

[19] https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series [accessed 1/11/2019].

[20] https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Stand ard_Project [accessed 30/10/2019].

[21] https://www.question-defense.com/2019/10/07/what-are-the-owasp-top-10-vulnerabilities,What Are The OWASP Top 10 Vulnerabilities?

[22] LARS LOFGREN, i2019. iWebsite Security Guide, Published on MARCH 13, 2019 -, https://www.quicksprout.com/website-security/ [accessed 27/10/2019]

[23] Philippe De Ryck,Lieven Desmet, Martin Johns and Frank Piessens,2014. Security assessment of the Web ecosystem, https://www.w3.org/2014/strint/papers/43.pdf. [accessed 30/11/2019]