वेब सुरक्षा

शालिनी लाम्बा[1], रिंकु रहेजा[2], सौरभ पति[3]
[1,2,3]असिस्टेंट प्रोफेसर, कम्प्यूटर विज्ञान विभाग
नेशनल पी0जी0 कॉलेज, लखनऊ–226001, उ0प्र0, भारत
shalinilamba22@gmail.com, rr_141085@yahoo.co.in,saurabhpati7@gmail.com

प्राप्त तिथि–30.07.2015, स्वीकृत तिथि–17.10.2015

पृथ्वी पर हम मानव सबसे बुद्धिमान प्राणी है, समय–समय पर हम मनुष्यों ने आग, पहिया, प्रिन्टिंग मशीन जैसी बड़ी–बड़ी खोजें की हैं, आज के युग की सबसे बड़ी खोज है– इन्टरनेट। आज हम सभी इस पर पूरी तरह निर्भर हैं, आज यह हमारा सबसे प्यारा और सबसे घनिष्ठ मित्र है। लेकिन वेब का उपयोग जितना हमारे कार्य को सहज बनाता है, उतना ही हमें स्वयं की सुरक्षा का ध्यान भी रखना होता है। आजकल लुटेरे बंदूकें लेकर बैंक नही लूटते, आज बस एक लैपटॉप और इंटरनेट कनेक्शन ही उनका हथियार होता है जिस तरह चोरों के हथियार बदल गये हैं, उसी तरह हमारे बचने के तरीके भी बदल गये है। अब देशों में भी सामान्य युद्ध नहीं होते, अब साइबर युद्ध हुआ करते हैं। एक दूसरे की गुप्त जानकारी उड़ाना अब हर देश का काम हो गया है। साइबर जगत में बढ़ते अपराध को देखते हुए आज वेब सुरक्षा की आवश्यकता बहुत बढ़ गयी है, आज हर कम्पनी में या हर एक संस्था में वेब सुरक्षा का एक अलग विभाग होता है, जो हर तरह से वेब सुरक्षा तथा इससे सम्बन्धित सभी तथ्यों पर ध्यान रखता है।

वेब सुरक्षा क्या है? "इंटरनेट पर अवांछित लोगों की पहुँच से स्वयं को बचाते हुए स्वयं को सुरक्षित करना ही वेब सुरक्षा है।" वेब सुरक्षा कम्प्यूटर विज्ञान का ऐसा क्षेत्र है जिसमें इंटरनेट से जुड़ी हर सुविधाओं एवं सुरक्षा का ध्यान रखा जाता है। वेब सुरक्षा में क्रॉस साइड स्क्रिपटिंग, एस0क्यू0एल0 इन्जेक्शन, डाटा ब्रीच, रिमोट अटैक, कोड इन्जेक्शन, बफर ओवर–फ्लो, मेमोरी करप्शन, पायरेसी जैसी समस्याओं को सुलझाया जाता है।

सामान्यतः यूजर कैसे हैक होता है? हमें रोज लोगों के, बैंकों के, सेना के डेटाबेस हैक होने या यूँ कहें कि किसी के भी डेटाबेस हैक होने की खबर मिलती रहती है। इन्हीं बढ़ते वेब हमलों से निपटने के लिए आज के यूजर को बहुत सावधानियाँ बरतनी पड़ती हैं। यूजर्स वेब का एक अति महत्वपूर्ण हिस्सा हैं, सारा काम, सारी डिजाइन, सारी प्रोग्रामिंग यूजर के लिए ही की जाती है। वेबसाइट्स और एप्लीकेशन्स् का मुख्य काम यूजर्स की आवश्यकताओं को पूर्ण करना ही है। इसीलिए हैकर्स का मुख्य टारगेट भी यूजर्स ही होते हैं। एंटीवायरस या इंटरनेट सुरक्षा का यूजर की डिवाइस पर ना होना ऑनलाइन अटैक से प्रभावित होने का सबसे बड़ा माध्यम है। जिन वेबसाइटों पर हैकिंग सम्बन्धी कोई भी प्रमाण या वायरस होता है, उसे इंटरनेट सुरक्षा प्रोग्राम रोक देते हैं तथा इनके अभाव में यूजर वाइरस युक्त फाइलों को अपने मोबाइल या कंप्यूटर में प्रवेश दे देता है। कुछ वाइरस जैसे रैट(रिमोट एक्सेस ट्रोजेन) स्वयं को यूजर के सिस्टम में आपलोड करके यूजर की हर जानकारी को हैकर तक पहुँचाते हैं या यू कहें कि यूजर की डिवाइस पर हैकर का पूरा कंट्रोल हो जाता है, हैकर की–लॉगर जैसी तकनीक का बड़े स्तर पर प्रयोग करता है और हर जानकारी उस तक आसानी से प्राप्त होती रहती है।

पब्लिक वाइ–फाई पर किसी भी वेबसाइट पर लॉग–इन करना घातक होता है। हैकर सामान्यतः किसी भी पब्लिक वाई–फाई(जो कि कम सुरक्षा वाला होता है) उसे हैक करके पहले स्वयं प्रवेश पाते हैं फिर उसमें जितने भी यूजर होते हैं या किसी टारगेटेड यूजर के डाटा पैकेट्स को कैप्चर कर लेता है और बाद में उसे डी–कोड करके यूजर की सारी जानकारी प्राप्त कर लेता है। मान लीजिए आप पब्लिक वाई–फाई में अपने क्रेडिट कार्ड से ऑनलाइन शॉपिंग कर रहे हैं तो अगर उस नेटवर्क में कोई हैकर हो तो हैकर बड़े आराम से आपके अकाउंट की सारी जानकारियां ले सकता है।

एक असुरक्षित नेटवर्क में हैकर यूजर की कोई भी डीटेल रियल टाइम में प्राप्त कर सकता है

किसी भी अवांछित वेबसाइट पर अकाउंट बनाकर अपनी बैंकिंग या सोशल नेटवर्किंग डीटेल्स देना भी यूजर के हैक होने की संभावना को बढ़ा देता है।

फिशिंग– यह हैकरों की पुरानी तथा प्रिय तकनीक है, इसमें हैकर यूजर को लोभ देकर उससे अपनी मनचाही लिंक खुलवाता है और उस लिंक से वो यूजर के डिवाइस पर या तो पूरा कंट्रोल कर सकता है या किसी फॉर्म से उसकी बैंक डीटेल या सोशल वेबसाइट्स की डीटेल्स को प्राप्त कर सकता है।

बगी ब्राउजर– वेब ब्राउजर एक अनेक प्रकार के सॉफ्टवेयर्स का मिश्रण है, जो की अपने आप में बहुत पेचीदा है और समय दर समय और भी पेचीदा होता जा रहा है, ये हैकरों के लिए बहुत अच्छा समाचार है अब वो और भी बग्स आसानी से इंजेक्ट कर सकेंगे। कभी कभी कुछ ब्राउजर ऐसी सुविधायें दे देते है, जिससे हैकिंग की संभावना अधिक बढ़ जाती है, जैसे गूगल क्रोम इनस्पेक्ट एलिमेंट नाम की सुविधा देता है जिससे कि कोई भी वेबसाइट का पूरा कोड देख सकता है, अगर वेब डेवलेपर चाह कर भी अपने कोड को नहीं छुपा सकता है। इससे हैकर को कोड समझ कर वेबसाइट पर हानिकारक लिंक्स डालने में सुविधा होती है। जब १९९० में टीम बनर्स–ली ने एच0टी0एम0एल0 को बनाया तब से कुछ दिनों तक सारी वेबसाइट्स एच0टी0एम0एल0 पर ही बनती रहीं हैं, लेकिन वेबसाइट्स को और आकर्षक बनाने के लिए सी0एस0एस0, जावास्क्रिप्ट, ऐजॉक्स जैसी स्क्रिप्टिंग लैंगवेजेस का प्रयोग होने लगा जिससे हैकर्स को बग्स को इनमें इनसर्ट करने की संभावना बढ़ गयी है। एक्टिव एक्स और प्लग–इन युक्त सॉफ्टवेयर डाउनलोड करने से भी हैकिंग का खतरा बढ़ जाता है, कम्प्यूटर की एक बड़ी दिक्कत यह है कि हम इसके सॉफ्टवेयर को प्रयोग करते समय स्वयं को सॉफ्टवेयर ऑनर के हाथ में दे देते है, हमें सॉफ्टवेयर के सारे विकल्प पालन करने होते हैं, कभी–कभी कुछ सॉफ्टवेर निर्माता सॉफ्टवेयर में हानिकारक कोड्स डाल देते हैं जिससे कि यूजर की गोपनीयता तथा जानकारी सुरक्षित नहीं रहती है।

हैकर यूजर से क्या चाहता है?

- यूजर के कम्प्यूटर पर पूरा एक्सेस।
- यूजर का आईडी पासवर्ड।
- वे यूजर के कम्प्यूटर की जानकारी को करेप्ट करना चाहते हैं।
- वे यूजर के कम्प्यूटर में स्टोर बैंकिंग डाटा और सॉफ्टवेयर का प्रयोग करना चाहते हैं।

वेब को सुरक्षित कैसे करें? वैसे तो वेब को सुरक्षित करना पूरी तरह से संभव नहीं है, हैकर्स कोई ना कोई रास्ता निकाल ही लेते हैं, जिससे वे हानि पहुँचा सकें, फिर भी कुछ ऐसे रास्ते हैं जिससे कि यूजर सुरक्षित रहेगा। डिवाइस में एक अच्छा एंटीवायरस होना आवश्यक है जो कि गलत लिंक्स को ब्लॉक करके उन्हें खुलने नहीं देता, जिससे की हैकिंग की संभावना और भी कम हो जाती है, यह एक फायरवॉल की तरह कार्य करता है, जिसमे बिना कोई सेटअप किए डाइरेक्ट रन होता है। केवल उन्हीं साफ्टवेयर का प्रयोग करें जिसके बारे में पूरी जानकारी हो, जिससे साफ्टवेयर में छुपे वाइरस या बग से बचा जा सकता है, सामान्यतः हैकर ही कुछ साफ्टवेयर के निर्माता होते है, और जैसे ही हम उन वाइरस युक्त साफ्टवेयर को अपने कम्प्यूटर में लोड कर लेते हैं, हम उनके शिकार हो जाते हैं इनसे बचने के लए हमें सोच समझ के सॉफ्टवेयर डाउनलोड करने चाहिये।

यूजर के द्वारा पब्लिक वाई–फाई का उपयोग करते समय उसे कोई भी ऑनलाइन पेमेंट या लॉगइन नही करना चाहिये, यदि यूजर का डाटा कोई देखेगा भी तो वह नॉर्मल डाटा होगा, जिससे यूजर को कोई हानि नहीं होगी। यदि ब्राउजर हमें किसी वेबपेज का डिजिटल सार्टिफिकेट नहीं दिखा रहा है तो हमें उसमें नही जाना चाहिये। फिशिंग से बचने के लिए हमें बिना जाने कोई भी लिंक नही खोलनी चाहिये। हमेशा एच0टी0टी0पी0एस0 युक्त लिंक ही खोलना चाहिये। अपने सभी अकाउंट्स के लिए मजबूत पासवर्ड लगायें, जिसमे अंक, स्पेशल सिंबल और अक्षर का मिश्रण हो।

हमें वेब जगत की दुनिया में आगे बढ़ते हुए, इस पर अपनी सुरक्षा का ध्यान रखते हुए अपनी सुरक्षा प्रणाली को और भी मजबूत करना होगा, वेब की कोई सीमा नहीं है इसीलिए हैकिंग की भी कोई सीमा नहीं है, तो हैकर्स भी अपना काम करते रहेंगे और हम भी उन्हें विफल करते रहेंगे।

सन्दर्भ

1. स्पाफोड, जेनी एवं गरफिन्केल, सिमसन(2001) वेब सिक्योरिटी प्राइवेसी एण्ड कॉमर्स, ओ–रैली मीडिया इंक।
2. https://en.wikipedia.org/