VEB-ILOVALARNI SUQULIB KIRISHGA TESTLASH (PENETRATION TESTING): AMALIY VOSITALAR VA EKSPLUATATSIYA JARAYONI

Xabibullayev Jahongirbek Doniyorbek o‘g‘li
Muhammad al-Xorazmiy nomidagi Toshkent
Axborot Texnologiyalari Universiteti assistenti
e-mail: j.xabibullayev@tuit.uz
Chunayev Norquvvat Eshquvat o‘g‘li
Muhammad al-Xorazmiy nomidagi Toshkent
Axborot Texnologiyalari Universiteti assistenti
e-mail: norkuvvatchunaev@gmail.com

Annotatsiya

Mazkur maqola veb-ilovalar va axborot tizimlarining xavfsizligini ta'minlashda muhim o‘rin tutuvchi “suqulib kirishga testlash” (penetration testing) jarayonlarini chuqur tahlil qilishga qaratilgan. Maqolada “axloqiy xakerlik” (ethical hacking) tamoyillari, testlash metodologiyalari (qora, kulrang va oq quti) hamda bu jarayonda qo‘llaniladigan ixtisoslashgan dasturiy vositalar (Nmap, Burp Suite, Gobuster, Metasploit, Hydra) batafsil yoritilgan. Shuningdek, haqiqiy zaifliklarni aniqlash mexanizmini ko‘rsatib berish maqsadida Nibbleblog CMS tizimi misolida RCE (Remote Code Execution) zaifligini amaliy ekspluatatsiya qilish, reverse shell (qaytarma qobiq) o‘rnatish va tizim ustidan nazoratni qo‘lga kiritish bo‘yicha bosqichma-bosqich amaliy ssenariy ishlab chiqilgan. Yakunda ushbu zaifliklarni bartaraf etish bo‘yicha texnik tavsiyalar berilgan.

Kalit so‘zlar: veb-ilovalar xavfsizligi, suqulib kirishga testlash (penetration testing), axloqiy xakerlik, kiberxavfsizlik, zaifliklarni aniqlash, ekspluatatsiya, qaytarma qobiq (reverse shell), xavfsizlik auditi, Nmap, Metasploit.

Kirish

Bugungi kunda davlat idoralari, moliya institutlari, yirik korporatsiyalar va hatto kichik biznes vakillari ham o‘z faoliyatlarini raqamli platformalar hamda veb-ilovalar orqali amalga oshirmoqda. Tizimlarning internet tarmog‘iga ochiqligi, ularga dunyoning istalgan nuqtasidan ulanish imkoniyati axborot qulayligini ta’minlash bilan birga, kiberjinoyatchilar uchun ham cheksiz hujum maydonini yaratib bermoqda.

Veb-ilovalarda saqlanadigan maxfiy ma’lumotlar, moliyaviy tranzaksiyalar va shaxsiy ma’lumotlarni himoya qilish maqsadida ishlab chiquvchilar turli xavfsizlik mexanizmlarini joriy etishadi. Biroq, inson omili, mantiqiy xatolar, yangilanmagan dasturiy ta'minotlar va arxitekturaviy kamchiliklar sababli tizimlarda “zaifliklar” (vulnerabilities) qolib ketishi tabiiy holatdir. Ushbu zaifliklarni real hujumchilar

aniqlamasidan oldin topish va bartaraf etishning eng samarali usuli bu – tizimni maxsus “suqulib kirishga testlash” (Penetration Testing yoki qisqacha Pen-testing) dan o‘tkazishdir.

Penetration testing – bu axborot tizimlarida, veb-ilovalarda va tarmoq infratuzilmasida mavjud xavfsizlik zaifliklarini aniqlash maqsadida ruxsat etilgan, qonuniy va xavfsiz muhitda o‘tkaziladigan simulyatsiya qilingan kiberhujum jarayonidir. U tizim egasining ruxsati bilan “axloqiy xakerlar” (white-hat hackers) tomonidan amalga oshiriladi. Maqsad – tizimni buzish emas, balki buzilish ehtimoli bor nuqtalarni ko‘rsatib, himoyani kuchaytirishdir.

Veb-ilovalarga suqulib kirish testlari tasodifiy harakatlar majmuasi emas, balki aniq xalqaro standartlar va metodologiyalar (masalan, PTES - Penetration Testing Execution Standard, OSSTMM, OWASP Testing Guide) asosida amalga oshiriladigan tizimli jarayondir. Tizim haqidagi boshlang‘ich ma’lumotlarning hajmiga qarab, testlash quyidagi uchta asosiy turga bo‘linadi:

1. Qora quti (Black Box) testlashi: Bu yondashuvda testerga nishon tizim haqida hech qanday oldindan ma’lumot (kod, arxitektura, IP manzillar ro‘yxati yoki parollar) berilmaydi. Tester xuddi oddiy tashqi tajovuzkor kabi faqat ochiq internet orqali o‘rganishni boshlaydi. Bu usul eng real hujum ssenariysini taqlid qiladi, lekin ko‘p vaqt talab etadi.

2. Oq quti (White Box / Clear Box) testlashi: Bu usulda tester tizimning to‘liq manba kodiga (source code), infratuzilma sxemalariga va administrator huquqlariga ega bo‘ladi. Maqsad eng chuqur va yashirin mantiqiy xatolarni qisqa vaqt ichida aniqlashdir.

3. Kulrang quti (Grey Box) testlashi: Yuqoridagi ikki usulning gibrid shakli. Tester tizim haqida qisman ma’lumotga (masalan, oddiy foydalanuvchi akkaunti yoki qisman hujjatlarga) ega bo‘ladi. Ko‘pincha tizim ichidagi foydalanuvchi o‘z vakolatlarini qanday oshirishi mumkinligini (Privilege Escalation) tekshirish uchun qo‘llaniladi.

Testlashning asosiy bosqichlari:

- *Axborot yig‘ish (Information Gathering / Reconnaissance):* Nishon haqida IP manzillar, domenlar, subdomenlar, ishlatilgan texnologiyalar haqida ma’lumot to‘plash.
- *Skanerlash va Enumiratsiya (Scanning and Enumeration):* Ochiq portlarni, xizmatlarni, yashirin papkalarni va xizmat versiyalarini aniqlash.
- *Zaifliklarni tahlil qilish (Vulnerability Analysis):* Topilgan ma’lumotlarni ma'lum bo‘lgan zaifliklar (CVE) bazalari bilan solishtirish.
- *Ekspluatatsiya (Exploitation):* Topilgan zaiflikdan foydalanib, tizimga ruxsatsiz kirishni amalga oshirish.

➢ *Post-Ekspluatatsiya (Post-Exploitation):* Tizimga kirgandan so‘ng, huquqlarni kengaytirish (root/admin olish), tarmoqning boshqa qismlariga o‘tish (pivoting) va o‘z izlarini tozalash.

➢ *Hisobot tayyorlash (Reporting):* Barcha topilmalar, ularning xavflilik darajasi va bartaraf etish usullari bayon qilingan rasmiy hujjat taqdim etish.

Amaliy testlashda qo‘llaniladigan maxsus dasturiy vositalar. Zamonaviy xavfsizlik tekshiruvlarini ixtisoslashgan dasturiy vositalarsiz tasavvur qilib bo‘lmaydi. Odatda bu vositalar xavfsizlik mutaxassislari uchun maxsus ishlab chiqilgan Kali Linux yoki Parrot Security OS kabi operatsion tizimlarda jamlangan bo‘ladi. Eng ko‘p ishlatiladigan vositalar quyidagilardir:

1. Nmap (Network Mapper) – Tarmoqni xaritalash, ochiq portlarni va xizmatlarni aniqlash uchun ishlatiladigan sanoat standarti. Nmap nafaqat ochiq portlarni topadi, balki TCP/IP paketlarini tahlil qilish orqali u yerda qaysi operatsion tizim (OS detection) va qaysi dastur qanday versiyada (Service detection) ishlayotganini aniqlay oladi.

2. Burp Suite – Veb-ilovalarni testlashda “de-facto” standart hisoblanadi. U foydalanuvchi brauzeri va veb-server o‘rtasida “Proxy” (vositachi) sifatida ishlaydi. Uning yordamida yuborilayotgan va kelayotgan HTTP so‘rovlarni ushlab qolish (Intercept), ularni o‘zgartirish va takroran yuborish (Repeater moduli), shuningdek avtomatlashtirilgan hujumlarni (Intruder) amalga oshirish mumkin.

3. Gobuster / Dirb – Veb-serverdagi yashirin kataloglar (papka) va fayllarni aniqlash uchun ishlatiladigan vosita. U “brute-force” (qo‘pol kuch) usulida ishlaydi: katta so‘zlar ro‘yxatidagi (wordlist) har bir so‘zni URL manzilga qo‘shib tekshiradi va serverdan qaytgan status kodiga qarab (200 OK, 403 Forbidden) resurs mavjudligini aniqlaydi.

4. SQLmap – Ma’lumotlar bazalariga SQL inyeksiya (SQLi) hujumlarini amalga oshirish va ulardagi ma’lumotlarni ajratib olish jarayonini avtomatlashtiruvchi kuchli vosita.

5. Metasploit Framework – Dunyodagi eng ommabop penetratsion test platformasi. U o‘zida minglab tayyor exploit'lar (zaiflikni ishga tushiruvchi kod), payload'lar (tizimga kirgach bajariladigan yuklama kod) va yordamchi modullarni jamlagan.

6. Hydra – Turli tarmoq xizmatlari (SSH, FTP, HTTP Login, RDP) parollarini lug‘at (dictionary attack) yoki qo‘pol kuch (brute-force) orqali buzishga qaratilgan juda tezkor vosita.

Amaliyotda zaifliklar qanday qidirilishi va ekspluatatsiya qilinishini ko‘rsatish maqsadida, muayyan maqsadli server (Target IP: 10.129.12.40) misolida to‘liq tsiklli (Full-cycle) hujum ssenariysini ko‘rib chiqilgan. Ushbu ssenariy ochiq kodli “Nibbleblog CMS” tizimidagi real zaiflikka asoslangan.

Hujumchi birinchi navbatda nishon mashinada qanday xizmatlar ishlayotganini bilishi kerak. Buning uchun Nmap vositasidan foydalaniladi.

Termialda quyidagi buyruq kiritiladi:

```
nmap -sC -sV -p- -T4 10.129.12.40
```

-sC (default skriptlarni ishga tushirish), -sV (xizmat versiyalarini aniqlash), -p- (barcha 65535 ta portni skanerlash).

Skanerlash natijasida ikkita ochiq port aniqlanadi:

- Port 22/tcp (SSH): OpenSSH 7.2p2 Ubuntu 4ubuntu2.8
- Port 80/tcp (HTTP): Apache httpd 2.4.18 (Ubuntu)

HTTPS (443 port) mavjud emas, demak tarmoqdagi barcha trafik ochiq matn (plaintext) ko‘rinishida uzatilmoqda. SSH 22-port ochiqligi e'tiborga olinadi, ammo hozircha parol yo‘qligi sababli asosiy e'tibor 80-portdagi veb-serverga qaratiladi.

Hujumchi brauzer orqali http://10.129.12.40 manziliga kiradi. Odatdagi “Hello World” kabi oddiy sahifa ochiladi. Sahifaning HTML manba kodi (View Page Source) o‘rganilganda, dasturchi tomonidan unutib qoldirilgan quyidagi izoh (comment) topiladi:

```
``
```

Ushbu ishora orqali /nibbleblog/ katalogiga o‘tiladi va u yerda to‘liq ishlashga tayyor veb-sayt (blog) ishlayotgani ma'lum bo‘ladi.

Saytning admin paneli va boshqa yashirin qismlarini topish uchun Gobuster vositasi yordamida kataloglarni brute-force qilinadi:

```
gobuster dir -u http://10.129.12.40/nibbleblog/ -w /usr/share/wordlists/dirb/common.txt
```

Gobuster quyidagi muhim kataloglarni topadi:

- ✓ /admin (Admin paneli, login sahifasi)
- ✓ /content (Foydalanuvchi yuklagan fayllar)
- ✓ /themes (Sayt mavzulari)
- ✓ /README (Tizim haqida ma’lumot)

Hujumchi topilgan http://10.129.12.40/nibbleblog/README faylini o‘qiydi. Ushbu faylda sayt dvijogi “**Nibbleblog 4.0.3”** ekanligi ochiq yozilgan bo‘ladi.

Tizim versiyasi ma’lum bo‘lgach, hujumchi Kali Linux’dagi ochiq ekspluatlar bazasidan (SearchSploit) ushbu versiyaga tegishli zaifliklarni izlaydi:

```
searchsploit Nibbleblog 4.0.3
```

Natija shuni ko‘rsatadiki, aynan *Nibbleblog 4.0.3* versiyasida *Arbitrary File Upload* (Foydalanuvchi fayllarini yuklashdagi zaiflik, CVE-2015-6967) mavjud bo‘lib, u bevosita *Remote Code Execution (RCE)* ga olib keladi.

Fayl yuklash zaifligidan foydalanish uchun admin paneliga kirish talab etiladi. Administrator login sahifasi /nibbleblog/admin.php manzilida joylashgan. Tester bu yerda standart parollarni (admin/admin) sinab ko‘rishi yoki oldindan topilgan/brute-force qilingan parollar orqali panelga kirishga muvaffaq bo‘ladi deb faraz qilaylik (masalan, admin:nibbles).

Tizimga kirgach, administrator interfeysidan “Plugins” bo‘limiga, so‘ngra “My Image” plaginiga o‘tiladi. Ushbu plagin orqali saytga rasm yuklash ko‘zda tutilgan.

Biroq, ushbu tizimda ishlab chiquvchilar yuklanayotgan fayl turini (fayl kengaytmasini) qat'iy tekshiradigan filtr o‘rnatishmagan. Shu bo‘shliqdan foydalanib, hujumchi rasm (masalan, .jpg yoki .png) o‘rniga, ichida zararli tizim buyruqlarini bajaruvchi PHP skript yozilgan shell.php faylini yuklaydi.

Yuklangan PHP fayl serverning quyidagi yashirin katalogida saqlanadi:

http://10.129.12.40/nibbleblog/content/private/plugins/my_image/image.php

(Tizim yuklangan faylning nomini avtomatik ravishda image.php *ga o‘zgartirgan bo‘ladi, lekin uning ichidagi zararli kod o‘zgarishsiz qoladi).*

Reverse Shell (qaytarma qobiq) – bu nishon kompyuter (server) tajovuzkorning kompyuteriga o‘zi faol ulanishni amalga oshiradigan masofaviy boshqaruv usulidir. Bu ko‘pincha Firewalldagi kiruvchi (inbound) cheklovlarni aylanib o‘tish uchun ishlatiladi, chunki firewallar odatda chiquvchi (outbound) ulanishlarga ruxsat beradi.

1. Tinglovchini ishga tushirish: Tajovuzkor o‘z kompyuterida (Kali Linux) Netcat vositasi yordamida kiruvchi ulanishlarni kutish uchun port ochadi:

nc -lvnp 1337

Yuklangan kodni (Payload) ishga tushirish: Tajovuzkor brauzer orqali boya yuklangan fayl manziliga murojaat qiladi:

http://10.129.12.40/nibbleblog/content/private/plugins/my_image/image.php.

2. Server ushbu PHP faylni o‘qiydi, ichidagi kodni ishga tushiradi va tajovuzkor ko‘rsatgan IP va 1337-portiga ulanish jo‘natadi.

3. Tizimni egallash: Tajovuzkorning terminalida ulanish qabul qilinadi. Endi hujumchi nishon serverda nibbler (yoki www-data) foydalanuvchisi huquqida Linux tizim buyruqlarini masofadan bemalol ishlata oladi. Bu kompyuterni to‘liq nazorat qilish (RCE) deganidir.

Ushbu nuqtadan boshlab hujumchi “Post-Ekspluatatsiya” bosqichiga o‘tishi, Linuxyadrosidagi zaifliklarni (masalan, Sudo misconfiguration, SUID bitlar) qidirib, oddiy nibbler foydalanuvchisidan “Root” (super-administrator) huquqlarigacha ko‘tarilishi (Privilege Escalation) mumkin.

Yuqoridagi ssenariyda ko‘rsatilgan kiberxavflar qanchalik xatarli bo‘lmasin, ularni to‘g‘ri sozlangan himoya arxitekturasi orqali to‘liq bartaraf etish mumkin. Amaliy test natijalari asosida quyidagi himoya choralarini qo‘llash tavsiya etiladi:

1. Dasturiy ta'minotlarni yangilash (Patch Management):

Eng katta xatolik – bu tizimda eskirgan va ma’lum zaifliklarga ega (CVE-2015-6967) bo‘lgan Nibbleblog 4.0.3 CMS’dan foydalanishdir. Tizim zudlik bilan eng so‘nggi va xavfsiz versiyaga yangilanishi, yoxud butunlay xavfsizroq alternativ CMS ga (masalan, oxirgi versiyadagi WordPress) o‘tkazilishi shart. Barcha server xizmatlari (Apache, OpenSSH, PHP) doimiy ravishda so‘nggi patchlar bilan yangilanib turishi kerak.

2. Fayl yuklash filtrlarini qat'iylashtirish (Input Validation & Sanitization):

“My Image” kabi plaginlarda mijoz tomonidan yuklanayotgan fayllarni qattiq nazorat qilish kerak. Fayl kengaytmasini (faqat .jpg, .png, .gif ga ruxsat berish - Whitelisting), MIME turini va fayl tarkibining haqiqatdan ham rasm ekanligini chuqur tekshirish zarur.

3. Yuklangan fayllarni xavfsiz saqlash va bajarilishini cheklash:

Fayllar yuklanadigan kataloglar (masalan, /content/private/) veb-serverning asosiy ildiz (Document Root) papkasidan tashqarida joylashishi maqsadga muvofiqdir. Shuningdek, Apache yoki Nginx konfiguratsiyasida ushbu papkalar ichidagi skriptlarning (PHP, Python) ishga tushirilishini qat'iyan taqiqlash (Disable Script Execution) talab etiladi.

4. Axborot sizib chiqishining oldini olish (Information Disclosure):

Sahifa manba kodida yashirin manzillarni izoh (comment) sifatida qoldirish o‘ta mas'uliyatsiz yondashuvdir. Mahsulotni ishlab chiqarish (production) muhitiga tushirishdan oldin bunday izohlar o‘chirib tashlanishi kerak. Shuningdek, README, CHANGELOG kabi tizim versiyasini oshkor qiluvchi fayllarga tashqi tomondan murojaat qilish server konfiguratsiyasi orqali taqiqlanishi (403 Forbidden) shart.

5. Kataloglarni ko‘rishni taqiqlash (Disable Directory Listing):

/themes kabi jildlarda Directory Listing (papkadagi barcha fayllar ro‘yxatini brauzerda ko‘rsatish) funksiyasi ochiq qolgan. Apache sozlamalaridan Options - Indexes direktivasini qo‘shish orqali bu xavf yopilishi kerak.

6. Xavfsiz ulanishni ta'minlash (HTTPS va SSH):

Tarmoq trafigini himoyalash uchun zudlik bilan 80-portdagi HTTP o‘rniga 443-portda shifrlangan HTTPS protokoli (SSL/TLS sertifikati bilan) joriy etilishi kerak. SSH (22-port) xavfsizligini oshirish uchun parol orqali ulanishni o‘chirib, faqatgina ochiq kalitlar (SSH Key-based Authentication) orqali ulanishga ruxsat berish tavsiya qilinadi.

Xulosa

Axborot texnologiyalari jadal taraqqiy etayotgan hozirgi davrda, faqatgina funksional va chiroyli veb-ilova yaratish bilan cheklanib qolish katta risklarni o‘zida yashiradi. Penetration testing – bu axborot xavfsizligini ta’minlashdagi faol himoya usullaridan biri bo‘lib, u kiberjinoyatchilarning ongini va xatti-harakatlarini modellashtirish orqali tizimning real bardoshliligini sinovdan o‘tkazadi.

Ushbu maqolada keltirilgan Nibbleblog CMS misolidagi ssenariy shuni yaqqol ko‘rsatadiki, hatto bitta kichik tekshirilmagan plagin (“My Image”) va versiyasi eskirgan tizim butun serverning to‘liq egallanishiga (Reverse Shell va RCE) olib kelishi mumkin. Shu sababli, suqulib kirishga testlash jarayonlarini tizimni ishlab chiqish (SDLC) va joriy etishning barcha bosqichlariga kiritish, muntazam ravishda xavfsizlik auditlarini o‘tkazish, hamda mutaxassislarni ilg‘or vositalar (Nmap, Burp Suite, Metasploit) bilan ta’minlash zamonaviy xavfsizlik strategiyasining poydevori bo‘lmog‘i lozim. Tashkilotlar shuni anglashlari kerakki, xavfsizlik bu bir martalik natija emas, balki izchil va to‘xtovsiz davom etadigan jarayondir.

Foydalanilgan adabiyotlar

1. Stuttard D., Pinto M. *The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws.* 2-nashr. Indianapolis: Wiley Publishing, 2011. – 912 bet.

2. OWASP Foundation. *OWASP Top 10:2021 – The Ten Most Critical Web Application Security Risks.* (Veb-ilovalar xavfsizligi bo‘yicha eng muhim xalqaro standart hujjat). https://owasp.org/www-project-top-ten/

3. PortSwigger Ltd. *Burp Suite Documentation and Web Security Academy.* (Veb-ilovalar xavfsizligini testlash vositalari va amaliyotlari). https://portswigger.net/burp/documentation

4. OffSec (Offensive Security). *Kali Linux Documentation.* (Suqulib kirish testlari uchun mo‘ljallangan ixtisoslashgan OS va uning ichki vositalari, jumladan Nmap, Metasploit, Gobuster bo‘yicha qo‘llanmalar).

5. TryHackMe. *Cyber Security Training Platform.* (Nibbleblog kabi haqiqiy zaif tizimlarda RCE va Reverse Shell modellashtirish uchun ta'limiy platforma resurslari). https://tryhackme.com/

6. Fielding R., Reschke J. *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing.* RFC 7230. IETF, 2014. (HTTP protokoli, so‘rovlarni boshqarish va marshrutlash standartlari). https://datatracker.ietf.org/doc/html/rfc7230