<table>
<tr><td rowspan="2">Application Security</td><td colspan="3">S07 T02</td></tr>
<tr><td colspan="3">Understanding common application vulnerabilities</td></tr>
<tr><td rowspan="3">امنیت نرم‌افزارها یکی از جنبه‌های حیاتی در مدیریت سرورهای لینوکسی است. درک و شناخت آسیب‌پذیری‌های رایج نرم‌افزارها می‌تواند به مدیران سیستم کمک کند تا اقدامات موثری برای محافظت از سرورها و داده‌های حساس انجام دهند. در این مقاله، به بررسی برخی از آسیب‌پذیری‌های رایج نرم‌افزارها و روش‌های کاهش آن‌ها می‌پردازیم.</td><td>بعد از</td><td colspan="2">Minimizing software to reduce vulnerability</td></tr>
<tr><td>قبل از</td><td colspan="2">Deploying application firewalls</td></tr>
<tr><td>پیاده سازی عملی: خیر</td><td>پژوهشی: بله</td><td>راهنمای عملی: خیر</td></tr>
</table>

درک آسیب‌پذیری‌های رایج نرم‌افزارها در لینوکس

امنیت نرم‌افزارها یکی از جنبه‌های حیاتی در مدیریت سرورهای لینوکسی است. درک و شناخت آسیب‌پذیری‌های رایج نرم‌افزارها می‌تواند به مدیران سیستم کمک کند تا اقدامات موثری برای محافظت از سرورها و داده‌های حساس انجام دهند. در این مقاله، به بررسی برخی از آسیب‌پذیری‌های رایج نرم‌افزارها و روش‌های کاهش آن‌ها می‌پردازیم.

آسیب‌پذیری‌های رایج نرم‌افزارها

1. **SQL Injection**

تزریق SQL یکی از آسیب‌پذیری‌های رایج در برنامه‌های وب است که به مهاجم اجازه می‌دهد تا دستورات SQL مخرب را به پایگاه داده ارسال کند. این آسیب‌پذیری می‌تواند منجر به دسترسی غیرمجاز به داده‌ها، تغییر داده‌ها و حتی حذف آن‌ها شود.

2. **اجرای کد از راه دور (Remote Code Execution)**:

آسیب‌پذیری اجرای کد از راه دور به مهاجم اجازه می‌دهد تا کد مخرب را بر روی سرور اجرا کند. این آسیب‌پذیری معمولاً به دلیل نقص در نرم‌افزار یا کتابخانه‌های استفاده شده رخ می‌دهد و می‌تواند منجر به کنترل کامل سرور توسط مهاجم شود.

3. **XSS (Cross-Site Scripting)**:

حملات XSS زمانی رخ می‌دهد که مهاجم کدهای مخرب جاوااسکریپت را در صفحات وب تزریق می‌کند. این حملات می‌توانند منجر به سرقت اطلاعات کاربران، تغییر محتوای صفحه و اجرای کدهای مخرب در مرورگر کاربران شوند.

4. **CSRF (Cross-Site Request Forgery)**:

در حملاتCSRF ، مهاجم کاربر را فریب می‌دهد تا یک درخواست مخرب را به یک برنامه وب ارسال کند. این حملات می‌توانند منجر به انجام عملیات ناخواسته مانند تغییر تنظیمات حساب کاربری یا انجام تراکنش‌های مالی بدون اطلاع کاربر شوند.

5. **آسیب‌پذیری‌های ارتقاء سطح دسترسی (Privilege Escalation)**:

این نوع آسیب‌پذیری‌ها به مهاجم اجازه می‌دهند تا سطح دسترسی خود را از کاربر عادی به کاربر ریشه (root) یا مدیر سیستم ارتقاء دهد. این امر می‌تواند منجر به کنترل کامل سیستم و دسترسی به تمامی داده‌ها شود.

روش‌های کاهش آسیب‌پذیری‌ها

۱. **استفاده از ورودی‌های معتبر** :همیشه ورودی‌های کاربران را بررسی و اعتبارسنجی کنید. استفاده از پارامترهای آماده‌سازی شده (prepared statements) در دستورات SQL می‌تواند از تزریق SQL جلوگیری کند.

```
// نمونه‌ای از پارامترهای آماده‌سازی شده در PHP

$stmt = $conn->prepare("SELECT * FROM users WHERE username = ?");

$stmt->bind_param("s", $username);

$stmt->execute();
```

۲. **بروزرسانی منظم نرم‌افزارها** :نرم‌افزارها، سیستم‌عامل و کتابخانه‌های استفاده شده را به طور منظم بروزرسانی کنید تا از آخرین پچ‌های امنیتی بهره‌مند شوید.

۳. **استفاده از فایروال‌های برنامه‌های وب (WAF)**: فایروال‌های برنامه‌های وب می‌توانند ترافیک ورودی را بررسی و حملات رایج مانند XSS و SQL Injection را مسدود کنند.

٤. **استفاده از مکانیزم‌های احراز هویت و مجوز دهی قوی** :از مکانیزم‌های احراز هویت دو مرحله‌ای (2FA) و مجوز دهی دقیق برای کنترل دسترسی کاربران استفاده کنید.

۵. **پیاده‌سازی سیاست‌های امنیتی محتوا (CSP):** سیاست‌های امنیتی محتوا می‌توانند به جلوگیری از حملات XSS کمک کنند.

```
Content-Security-Policy: default-src 'self'; script-src 'self'
https://trusted.cdn.com;
```

نتیجه‌گیری

شناخت آسیب‌پذیری‌های رایج نرم‌افزارها و اتخاذ تدابیر مناسب برای کاهش این آسیب‌پذیری‌ها یکی از اصول اساسی در امنیت نرم‌افزارها در سرورهای لینوکسی است. با استفاده از روش‌ها و ابزارهای مناسب، می‌توان از نفوذهای غیرمجاز جلوگیری کرد و امنیت سیستم را به طور قابل توجهی افزایش داد. آشنایی و پیاده‌سازی صحیح این روش‌ها به مدیران سیستم کمک می‌کند تا از داده‌های حساس خود محافظت کرده و از عملکرد بهینه سرورهای خود اطمینان حاصل کنند.

منابع و ارجاعات

- https://roadmap.sh/linux
- https://roadmap.sh/r/general-linux-server-hardening