مبانی امنیت اطلاعات

تمرین اول – مفاهیم امنیت

سوال اول

CVE-2022-23912

- **شرح مختصر آسیب پذیری**: افزونه Testimonial WordPress Plugin قبل از ورژن 1.4.7 قبل از خروجی افزونه، پارامتر id را حذف نمیکرد که منجر به یک کد XSS می شد.
- **ورژن و نوع سیستم تحت تاثیر**: ورد پرس های پایین تر از پرژن 1.4.7 (خود این ورژن محسوب نمیشود)
- **بسته یا برنامه حاوی آسیب پذیری**: افزونه ورد پرس
- **پیچیدگی حمله**: ۶.۱ - متوسط
- **تاثیر آسیب پذیری بر روی صحت، محرمانگی و دسترسی پذیری**: با حمله XSS هر سه میتوانند مورد آسیب پذیری قرار گیرند.

CVE-2022-25015

- **شرح مختصر آسیب پذیری**: یک آسیب پذیری XSS در Ice Hrm 30.0.0 به مهاجمان اجازه میدهد تا کوکی ها را از طریق یک محموله دستکاری شده که در قسمت First Name درج شده است، بدزدند.
- **ورژن و نوع سیستم تحت تاثیر**: Ice Hrm 30.0.0.OS
- **بسته یا برنامه حاوی آسیب پذیری**: اسکریپت از پیش ذخیره شده XSS
- **پیچیدگی حمله**: ۵.۴ - متوسط
- **تاثیر آسیب پذیری بر روی صحت، محرمانگی و دسترسی پذیری**: محرمانگی

CVE-2022-0377

- **شرح مختصر آسیب پذیری**: افزونه Crazy Bone ورد پرس نام کاربری ثبت شده هنگام ورود به سایت را در داشبورد برگردانده که میتواند منجر به XSS بدون احراز هویت شود
- **ورژن و نوع سیستم تحت تاثیر**: ورد پرس های پایین تر از پرژن 0.6.0 (خود این ورژن محسوب میشود)
- **بسته یا برنامه حاوی آسیب پذیری**: فرم ورود سایت
- **پیچیدگی حمله**: ۶.۱ - متوسط
- **تاثیر آسیب پذیری بر روی صحت، محرمانگی و دسترسی پذیری**: محرمانگی

CVE-2022-23911

- **شرح مختصر آسیب پذیری**: افزونه ورد پرس Testimonials پارامتر id را چک نکرده و در کد SQL لحاظ میکند که باعث میشود امکان SQL Injection پیش بیاید.
- **ورژن و نوع سیستم تحت تاثیر**: ورد پرس های پایین تر از پرژن 1.4.7 (خود این ورژن محسوب نمیشود)
- **بسته یا برنامه حاوی آسیب پذیری**: افزونه Testimonials
- **پیچیدگی حمله**: ۷.۲ - حساس
- **تاثیر آسیب پذیری بر روی صحت، محرمانگی و دسترسی پذیری**: محرمانگی

مبانی امنیت اطلاعات

تمرین اول – مفاهیم امنیت

CVE-2022-25412

- **شرح مختصر آسیب پذیری**: نرم افزار Maxsite CMS چند آسیب پذیری پاک کردن فایل ها از طریق admin_page/all-files-update-ajax.php/ و پارامتر های پاک کردن های فایل
- **ورژن و نوع سیستم تحت تاثیر**: maxsite_cms:108
- **بسته یا برنامه حاوی آسیب پذیری**: all-files-update-ajax.php
- **پیچیدگی حمله**: ۸.۱ - حساس
- **تاثیر آسیب پذیری بر روی صحت، محرمانگی و دسترسی پذیری**: دسترسی پذیری

سوال دوم

- **پیشگیری از حمله از تشخیص و بازیابی مهمتر باشد**: فاش شدن اطلاعات لاگین کاربران – سیستم دفاعی و موشک ها
- **تشخیص حمله از پیشگیری و بازیابی مهمتر باشد**: حفاظت از مدارک مهم در اتاق عمل – زمان کافی برای صحت سنجی اجازه افراد وجود ندارد ولی تیم امنیتی میتواند بعدا دسترسی ها را کنترل کند
- **بازیابی وضعیت بعد از حمله از پیشگیری و تشخیص مهمتر باشد**: سیستم های بانک که موجودی حساب ها بعد از هک شدن قابل بازیابی باشد

سوال سوم

موارد زیادی وجود دارد. برای مثال فاش شدن الگوریتم رمزنگاری پیام های بین دو نفر میتواند منجر شود تا Man in the Middle بتواند محتوای پیام را دستکاری کند. در اینجا فاش شدن الگوریتم نقض محرمانگی از سوی برنامه پیام رسانی است و تغییر محتوای پیام نقض صحت.

سوال چهارم

	Traffic Analysis	Change of Content	DoS
Data Origin Auth		Y	
Access Control Auth	Y		Y
Confidentiality		Y	
Availability	Y		Y

سوال پنجم

	Traffic Analysis	Change of Content	DoS
Data Integrity		Y	
Access Control	Y		Y
Routing Control	Y		Y
Digital Signature		Y	

مبانی امنیت اطلاعات

تمرین اول – مفاهیم امنیت

سوال ششم

استفاده از Ip Spoofing در حملات DoS دلایل زیادی دارد. از جمله:

- حفاظت از هویت هکر توسط مقامات، به گونه ای که از botnet ها استفاده میکنند. Botnet ها دستگاه های از پیش هک شده ای است که به صورت remote کنترل میشوند.
- عبور از لیست سیاه هایی که توسط سایت ها نوشته میشود، زیرا با این روش میتوان از نقاط مختلف حملات را انجام داد به گونه ای که لیست سیاه کارایی خود را از دست می دهد.
- با استفاده از این تکنیک تعداد درخواست های بسیار کوچک اما بسیار زیاد میتوان فرستاد به گونه ای که لایه های امنیتی قادر به پیش بینی و کنترل آنها نیستند. دلیل آن بالا بودن تعداد درخواست های متنوع از مکان های مختلف است.
- DNS Amplification: تعداد زیادی درخواست به DNS های unsecure ارسال می شود. هر درخواست به حجم ۶۰ بایت پاسخ ۴۰۰۰ بایت دارند. این منجر میشود مهاجم بتواند ترافیک را ۱ به ۷۰ افزایش دهد.
- Smurf Attack: درخواست ICMP که از نوع Echo است با ارسال به شبکه ای از دستگاه ها باعث میشود یک پاسخ از تمام دستگاه های شبکه بازگردانده شود. اگر فرض کنیم ۵۰ دستگاه متصل داریم، هر درخواست ۵۰ پاسخ دارد که با ضریب ۱ به ۵۰ افزایش میابد.