# به نام خدا

# محمدمهدی آقاجانی

# 9331056

# تمرین اول

# استاد : دکتر شهریاری

1 –

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| شناسه | توضیح | نوع سیستم عامل | برنامه حاوی | پیچیدگی حمله | تاثیر آسیب پذیری |
| CVE-2017-2282 | سرریز بافر در برخی ورژن های ویندوز باعث میشد که حمله کننده هر دستوری را بتواند در سیستم هدف اجرا نماید | WN-AX1167GR |  | پایین | تاثیر آن بر تمام سه فاکتور یاد شده بالا بوده است |
| CVE-2015-5059 | وقتی سطح دسترسی در حالت anybody در برنامه MantisBT قرار میگیرد به کاربر های تعیین هویت شده اجازه میدهد به طور ریموت هر پروژه پرایویت را مشاهده کنند | Network | mantisBT | بالا | محرمانگی را به شدت تحت تاثیر قرار میدهد ولی دو پارامتر دیگر را خدشه دار نمیکند |
| CVE-2017-12131 | اجازه حمله XSS در بخشی از یک پلاگین wordpress | Network | Easy Testimonials plugin 3.0.4 for WordPress | پایین | محرمانگی و صحت را به اندازه کمی تحت تاثیر قرار میدهد |
| CVE-2017-10829 | یک مسیر سرچ ناامن در یک ایزار پشتیبانی ریموت باعث میشد که حمله کننده اجازه دسترسی به فولدر های ناخواسته را داشته باشد. | Local network | Enkaku Support Tool | پایین | محرمانگی و صحت و دسترسی پذیری را به شدت تحت تاثیر قرار میدهد. |
| CVE-2017-1383 | برخی از سرور های IBM در هنگام پردازش XML ها این امکان را فراهم میکردند که حمله کننده از منابع زیادی از حافظه استفاده کن یا اطلاعات حساس را برداشت کند | network | IBM InfoSphere Information Server 9.1, 11.3, and 11.5 | پایین | موارد محرمانگی و دسترس پذیری را به شدت تحت تاثیر قرار میدهد ولی صحت را خیر |

2-

در حملاتی که منجر به نشت اطلاعات میشود پیشگیری بسیار مهم است زیرا اطلاعات اگر نشت بکند دیگر رفته و حمله اثرگذار بوده

در حالت هایی که سرویس از دسترس خارج میشود بازیابی بسیار مهم تر است.

در حالت هایی که اطلاعات تغییر داده میشوند تشخیص بسیار مهم میشود.

3- بله اگر حمله کننده بتواند به پوشه هایی که اجازه دسترسی به آن را ندارد دسترسی پیدا کند هم محرمانگی نقض شده و هم میتواند محتوا را تغییر دهد و صحت را مشکل دار کند.

4-

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| حملات سرویس ها | شنود | تحلیل ترافیک | جعل هویت | ارسال دوباره پیغام | دستکاری | منع خدمت |
| تصدیق اصالت |  |  | دارد | دارد |  |  |
| کنترل دسترسی | دارد | دارد |  | دارد | دارد | دارد |
| محرمانگی داده | دارد |  |  | دارد | دارد |  |
| صحت داده |  |  |  |  | دارد |  |
| عدم انکار |  |  | دارد | دارد |  |  |
| دسترس پذیری |  |  |  |  |  | دارد |

5-

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| حملات مکانیزم ها | شنود | تحلیل ترافیک | جعل هویت | ارسال دوباره پیغام | دستکاری | منع خدمت |
| کدگذاری | دارد |  |  | دارد |  |  |
| امضای دیجیتال |  |  | دارد | دارد | دارد |  |
| کنترل دسترسی | دارد |  |  | دارد | دارد | دارد |
| صحت کانال انتقالی | دارد | دارد |  | دارد | دارد |  |
| Traffic padding |  | دارد |  |  |  |  |
| کنترل مسیریابی | دارد | دارد |  |  | دارد |  |

6- از جعل آی پی در حمله منع خدمت استفاده میشود به این صورت که مبدا حمله تعداد زیادی آی پی جعلی تولید میکند تا اولا حمله نتواند سریعا بلاک شود و به نظر برسد که از منابع مختلفی حمله شده است و اینکه همچنین هویت خود و مبدا حمله را پنهان کند تا رهگیری آن سخت باشد.