پایگاه داده

٢ .حمله به پايگاه داده

١/٢ . چگونگي حمله injection Sql را توضيح دهيد.

روش این حمله به این صورت است که هکر در فرم های سایت، در فیلدی که باید اطلاعات خود را وارد کند، کد های مخرب SQL را وارد می کند و چون اين کد ها در زمان اجرا تفسير می شوند سيستم به جای اجرا کردن کد SQL اصلی، کد مورد نظر هکر را اجرا می کند.

به طور مثال در فیلد username چیزی به غیر از نام کاربری وارد شود مثلا hi’ or 1=1′

نوع اطلاعات ورودی در SQL Injection به نوع سرویس [هاستینگ](https://webramz.com/hosting) و دیتابیس بستگی دارد و هر دیتابیسی به یک سری کاراکترهای خاص حساس است.

٢/٢ . توضيح دهيد كه چرا فايروالهاي عام منظوره (مانند فايروال ويندوز) نمي توانند جلوي چنين حملهاي را بگيرند. با جستجو در اينترنت، گونه هايي از فايروال را توضيح دهيد كه ميتوانند مانع چنين حملاتي شوند.

WAF مخفف کلمه Web Application Firewall، یک سیستم فایروال پیشرفته می باشد که از وب اپلیکیشن در برابر موارد امنیتی همچون تهدیدات، بدافزارها و حملات مخرب محافظت می کند،

WAF این کار را با فیلتر و مانیتور کردن ترافیک های HTTP بین وب اپلیکیشن و اینترنت انجام می‌دهد.

فواید waf:

1. امنیت وب سایت را در مقابل حملات SQL injection، تامین می کند.

2. از وب سایت، در مقابل حملات Cross-site scripting و directory traversal محافظت می کند.

3. از حملات دستکاری پارامتر، کوکی و نشست جلوگیری می کند.

4. با شناسایی آبجکت ها از افشای اطلاعات جلوگیری می کند.

5. با بررسی گواهی SSL ترافیک های encrypt شده، از وب سایت، در برابر تهدیدات محافظت می کند.

6. امنیت وب سایت را در مقایل حملات DDoS تامین می کند.

7.از XML همراه با اعتبار سنجی SOAP messages و XPath، محافظت می کند.

8. دفاع در مقابل حملات injection را ارائه می دهد و مستندات XML ای که دارای محتوای مخرب می باشند را Block می کند.

عملکرد اصلی network firewall، کنترل سطح دسترسی، مانیتور کردن ترافیک وب در سراسر شبکه می باشد و همچنین Session های خروجی را مجاز می‌کند.

\* فایروال های شبکه (معمولی)، مکانیزمی جهت شناسایی و جلوگیری از تهدیدات ندارند.

\* فایروال های شبکه، فقط موارد محدودی از بدافزار ها، حملات و فعالیت های غیر مجاز را ارائه می دهند.

تفاوت میان nertwork firewallوwaf:

1. network firewall در لایه های 3 و 4، لایه بندی OSI کار می کند، در مقابل WAF در لایه های 3 و 7 فعالیت می کند.

2. network firewall در gateway لایه 3 پیاده سازی می شود ولی WAF را به صورت Reverse proxy پیاده سازی می کنند.

3. WAF و network firewall، هر دو کنترل دسترسی را با Port، Protocol و آدرس IP انجام می دهند.

4. network firewall، انواع پروتکل ها را پوشش می دهد،در مقابل WAF تنها پروتکل های

مبتنی بر وب مانند HTTP، HTTPs، XML و ... را پوشش می دهد.

5.network firewall، محافظت در مقابل حملات DDoS را بر روی لایه شبکه پشتیبانی می کند،ولی WAF آن را در لایه Application ارائه می دهد.

6. یک network firewall، حداقل محافظت ها را در قبال نرم افزار های کاربردی دارد در صورتی که WAF تمامی محافطت ها را در لایه Application پوشش می دهد.