禪

آموزش رایگان دوره CEH همگام با سرفصلهای بینالمللی - 43

آموزش CEH (هکر کلاه سفید): هکرها چگونه به برنامههای وبمحور حمله میکنند؟

C|EH ™
CERTIFIED ETHICAL HACKER

تضمین این موضوع که یک برنامه وب در امنیت قرار دارد، برای اغلب طراحان و توسعهدهندگان چالشبرانگیز است، زیرا آنها بهطور معمول تحت فشار قرار دارند تا برنامه را برای انتشار در اسرع وقت آماده کنند. به همین دلیل گاهی اوقات امنیت قربانی میشود. یکی از راههای ساخت برنامههای بهتر وب، توجه به امنیت از همان ابتدای کار است. نکته مهم دیگری که باید به آن دقت کرد ارزیابی کدهای نهایی است. اگر کد منبع در دسترس است، میتوان از اسکنرهای کد منبع برای شناسایی آسیبپذیری در کدهای اصلی استفاده کرد. اسکنر کدهای اصلی میتواند آسیبپذیریهایی از قبیل سرریز بافر، شرایط چالشبرانگیز، پارامترهایی که باعث ترفیع امتیاز میشوند را تشخیص دهد.

برای مطالعه قسمت قبل آموزش رایگان دوره CEH اینجا کلیک کنید.

ابزارهای مختلفی برای انجام تزریق SQL، دستکاری کوکیها، ایجاد مشکلات سرریز بافر و سایر حملات در دسترس هستند. اجازه دهید به نحوه کار ابزار Burp Proxy نگاهی داشته باشیم. تصویر زیر رابط کاربری ابزار فوق را در زمان تعامل با مکانیزم احراز هویت نشان میدهد.

burp suite professional v1.4.03 - licensed to PortSwigger
burp intruder repeater window about
target proxy spider scanner intruder repeater sequencer decoder comparer options alerts
intercept options history
forward drop intercept is on action
raw params headers hex
POST /auth/390/NewUser.ashx HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer:NewUser.ashx HTTP/1.1
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 6.1; WOW64; Trident/5.0)
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: 2f2597293dc2
Content-Length: 82
Proxy-Connection: Keep-Alive
Pragma: no-cache
Cookie: SessionId__990=DEEF029647623A7D6E1D7DE7596D0440D
realname=dad&username=dad&userrole=admin&password=123&confirmpassword=123
0 matches

.OWASP ZAP .

Session Properties
Session
General
Exclude from Proxy
Exclude from Scanner
Exclude from Spider
Contexts
1:Default Context
1: Include in Context
1: Exclude from Context
1: Structure
1: Technology
1: Authentication
1: Users
1: Forced User
1: Session Management
1: Authorization
1: Access Control
1: Alert filters
Monitor Clients
Exclude from WebSockets
1: Authentication
This panel allows you to configure the authentication scheme used for this Context.
Currently selected Authentication method for the Context:
Form-based Authentication
Configure Authentication Method
Login Form Target URL *:
http://localhost:8080/login.jsp
Select...
Login Request POST Data (if any):
username={%username%}&password={%password%}
Username Parameter *:
Password Parameter *:
username
password
The username and password fields will be replaced, during authentication, with the username and password corresponding to application's users.
Regex pattern identified in Logged In response messages:
Regex pattern identified in Logged Out response messages:
\QLogin\E
Cancel
OK

.RFC 5216 CEH

ابزارهایی که برای پیدا کردن آسیبپذیریها در دسترس قرار دارند به موارد زیر میتوان اشاره کرد :

- Flawfinder: یک برنامه نوشته شده به زبان پایتون است که با تحلیل کدهای اصلی یک برنامه به جستوجوی نقصهای امنیتی احتمالی یک برنامه پرداخته و معایب امنیتی که باعث بروز ریسکهای خطرناک میشوند را نشان میدهد .

- Rough Auditing Tool for Security : یک برنامه نوشته شده به زبان سی است که شامل مجموعهای از خطمشیهای خارجی XML است که برای هر زبان اعمال میشود . این نرمافزار میتواند نرمافزارهای نوشته شده به زبانهای PHP ، Perl ، C ++ ، C و Python را برای آسیبپذیریها و سرریزهای احتمالی بافر اسکن کند.

- StackGuard: میزان آسیبپذیری نرمافزارها در خصوص حملات stackmashing را بررسی میکند . حملات Stack-Smash یک مشکل رایج و بزرگ در برنامههای لینوکسی و ویندوزی است . پس از کامپایل برنامهها توسط StackGuard آنها تا حد زیادی در برابر حملات سرریز بافر مصون میشوند .

اگر کد منبع در دسترس نباشد، بازهم این امکان وجود دارد که از اسکنرهای سطح برنامه استفاده کرد . اسکنرهای سطح برنامه، به کارشناسان امنیتی اجازه میدهند تا برنامهها یا مؤلفههای به شیوه دیگر ارزیابی کنند . ا زجمله این اسکنرها به موارد زیر میتوان اشاره کرد :

- Whisker: یکی از قدیمیترین اسکنرهای ویژه برنامههای وب است که هنوز هم کاربرد دارد . ویسکر میتواند آسیبپذیریهای Common Gateway Interface (CGI) را بررسی کند . همچنین دارای مستندات کاربردی است که پیشنهاد میشود به دقت بررسی شوند. CGI یکی از مخاطراات بالقوه پیرامون برنامههای تحت وب است که باعث میشود اطلاعات سیستم که باید محرمانه نگه داشته شوند، نشت پیدا کرده و به کاربران از راه دور اجازه میدهد دستورات مخرب را اجرا کنند . ویسکر نیازمند پرل (Perl) است، بنابراین اگر قصد استفاده از آنرا دارید، مطمئن شوید که محیط پرل در دسترس باشد .

- N-Stalker: این ابزار ارزیابی نرمافزارها مبتنی بر رابط کاربری گرافیکی است و دارای یک بانک اطلاعاتی گسترده با بیش از 30،000 آسیبپذیری است. ابزار فوق پس از تحلیل نرمافزارها و شناسایی مشکلاتی با برچسبزنی آنرها به شکل تهدید زیاد، متوسط یا کم گزارش ساختیافتهای در اختیار مدیران قرار میدهد .

- WebInspect: یکی دیگر از ابزارهای پویش آسیبپذیریهای برنامههای وب است که میتواند بیش از 1500 آسیبپذیری مرتبط با وبسرورها و برنامههای شناخته شناخته شده را اسکن کند و رمزهای عبور ضعیف را شناسایی کند.

- Nikto: یک برنامه آماده بهکار و ساده برای استفاده است که آسیبپذیریهای برنامههای وب را شناسایی کرده و سرعت زیادی دارد . نرمافزار فوق قابلیت پویش پورتهای اساسی با هدف شناسایی پورتهای باز روی وبسرورها را دارد .

- AppDetectivePRO: این اسکنر در سطح برنامه تستهای نفوذ و ممیزی انجام داده و از دید یک هکر برنامهها را ارزیابی میکند . نرمافزار فوق نیازی به مجوزهای داخلی ندارد و با اجرای پرسوجو روی سرور میتواند اطلاعاتی درباره پایگاه دادهای که در حال اجرا است، مانند نسخه در حال استفاده را بهدست آورد. تست حسابرسی میتواند هر تعداد ضعف امنیتی را روی سرور شما، از رمزهای از دست رفته گرفته تا شناسایی حسابهای کاربری و وصلههای امنیتی که از دست رفته و نصب نشدهاند را تشخیص دهد .

یکی دیگر از تکنیکهایی که میتواند در ارتباط با یک برنامه کاربردی استفاده شود، فازی است . Fuzzing، همچنین به عنوان تست جعبه سیاه شناخته میشود. یک روش تست نرمافزاری است که دادههای نامعتبر، غیر منتظره یا تصادفی را به ورودیهای یک برنامه کامپیوتری ارائه میدهد تا وضعیت برنامه در ارتباط با قفل شدن، نمایش یک پیغام خطای ناگهانی و خاتمه برنامه و هرگونه فعالیت نامعتبری را را شناسایی کند .

تزریق کد **SQL**

حملات تزریق کد اسکیوال (SQL Injection Attacks) یکی دیگر از تهدیدات جدی پیرامون وبسایتهای یا برنامههای تحت وب هستند که از بانکهای اطلاعاتی استفاده میکنند . در روش فوق ممکن است کدهای مخرب یا اسکریپتهایی داخل محاورهای موجود وارد شده و اجرا شوند . کدهای مخرب با هدف آشکارسازی یا دستکاری دادههایی که در جداول درون پایگاه داده ذخیره شدهاند اجرا میشوند . تزریق SQL یک حمله قدرتمند و خطرناک است. در حمله فوق نقصها و آسیبپذیریهای درون یک وبسایت یا برنامه شناسایی میشود . فلسفه تزریق کد اسکیوال اجرای دستوراتی با هدف افشای اطلاعات حساس پایگاه داده است . به همین دلیل یکی از خطرناکترین بردارهای حمله پیرامون برنامههای تحت وب است .

دامنه انجام حملات تزریق **SQL**

تزریق SQL میتواند تهدید بزرگی برای وبسایتها یا برنامههایی باشد که از بانکهای اطلاعاتی استفاده میکنند . برای پیشگیری از بروز یک چنین حملاتی لازم است طراحان برنامههای وبمحور به یکسری موارد مهم دقت کنند . هکرها از انجام یک چنین حملاتی به دنبال اهدف زیر هستند :

دور زدن تأیید اعتبار

افشای اطلاعات حساس

به خطر انداختن یکپارچگی دادهها

پاک کردن پایگاه داده

اجرای کد از راه دور

محاورههای **SQL** چگونه کار میکنند؟

محاورههای SQL روی سرور اجرا میشوند و نتیجه در قالب پاسخ بازگردانده میشوند . به عنوان مثال، محاوره SQL درخواستی را برای سرور ارسال میکند .

[SELECT * FROM [Orders

دستور فوق تمام اطلاعات ذخیره شده در جدول "سفارشات" پایگاه داده را نشان میدهد . اگر سازمانی سوابق سفارشات خود را در یک پایگاه داده نگهداری کند و از تهمیدات خاصی برای ایمنسازی بانک اطلاعاتی استفاده نکرده باشد، یک چنین دستوری تمامی اطلاعات درون جداول بانک اطلاعاتی را استخراج میکند .

محاوره حذف **SQL**

فرمان DELETE برای حذف رکوردهای موجود در یک جدول بانک اطلاعاتی استفاده میشود . برای درک بهتر این موضوع، جدول "مشتریان" در یک پایگاه داده را در نظر بگیرید . اطلاعات زیر جدول "مشتریان" به شرح زیر است:

CustomerID	CustomerName	City
1	Maria Anders	London
2	Alfreds Futterkiste	Prague
3	Elizabeth Brown	Paris
4	Ana Trujillo	New York
5	Thomas Hardy	Boston

اجرای فرمان delete به شرح زیر باعث حذف یک رکورد اطلاعاتی میشود .

```
DELETE FROM Customers
```

```
;'WHERE CustomerName='Alfreds Futterkiste
```

اکنون جدول بانک اطلاعاتی به صورت زیر است :

CustomerID	CustomerName	City
1	Maria Anders	London
3	Elizabeth Brown	Paris
4	Ana Trujillo	New York
5	Thomas Hardy	Boston

دستورات پرسوجو SQL زیادی وجود دارد که همراه با فرمان Delete قابل استفاده هستند که میتوان از آنها به شکل موثری در فرآیند تزریق کد استفاده کرد .

محاوره بهروزرسانی **SQL**

فرمان UPDATE برای اصلاح رکوردی در یک جدول استفاده میشود . به مثال زیر دقت کنید :

```
UPDATE Customers
```

```
'SET ContactName = 'IPSpecialist, City= 'Frankfurt
```

```
;WHERE CustomerID = 1
```

فرمان فوق باعث میشود تا جدولی به شرح زیر داشته باشیم :

CustomerID	CustomerName	City
1	IPSpecialist	Frankfurt
3	Elizabeth Brown	Paris
4	Ana Trujillo	New York
5	Thomas Hardy	Boston

ابزارهای تزریق کد **SQL**

ابزارهای مختلفی برای تزریق کد SQL در دسترس است که از آن جمله به موارد زیر میتوان اشاره کرد :

BSQL Hacker

Marathon Tool

SQL Power Injector

Havij

روشهای مختلف تزریق کد

تزریق SQL را میتوان در سه دسته اصلی زیر طبقهبندی کرد .

1. In-band SQLi
2. Inferential SQLi
3. Out-of-band SQLi

گروه اول، تزریق کد به In-Band SQL□□□□

تزریق کد به شیوه In-Band شامل تکنیکهای تزریقی است که از کانال ارتباطی برای انجام حمله و جمعآوری اطلاعات پاسخ استفاده میکند . تکنیکهای تزریق In-Band موارد زیر را شامل میشوند :

1. Error-based SQL Injection
2. Union based SQL Injection

حملات تزریق کد مبتنی بر خطا

تزریق مبتنی بر خطا یکی در زیرمجموعه تکنیکهای in-band قرار میگیرد . حمله فوق بر مبنای پیغامهای خطایی که از جانب سرور بانک اطلاعاتی منتشر میشود و اطلاعاتی که در ارتباط با ساختار بانک اطلاعاتی بهدست میآید پیادهسازی میشود . حمله تزریق SQL مبتنی بر خطا موثرترین ابزاری است که هکرها برای سرشماری یک بانک اطلاعاتی از آن استفاده میکنند . پیامهای خطا در مرحله توسعه برای عیبیابی مشکلات مفید هستند. این پیامها باید هنگام فعال کردن وبسایت یا یک برنامه تحت وب غیرفعال شوند. تزریق SQL مبتنی بر خطا بر مبنای روشهای زیر پیادهسازی میشود :

System Stored Procedure

End of Line Comment

Illegal / Logically incorrect Query

Tautology

تزریق کد Union SQL

تزریق کد Union SQL یکی دیگر از تکنیکهای زیرمجموعه In-Band است که سعی میکند از عملگر UNION برای ترکیب نتایج دو یا چند فرمان SELECT در قالب یک نتیجه واحد استفاده کند .

```
SELECT <column_name(s)> FROM <table_1>

UNION

SELECT <column_name(s)> FROM <table_2>;
```

گروه دوم تزریق کد به شیوه Inferential SQL

در تزریق کد به شیوه استنتاجی که گاهی اوقات تزریق کد Blind Injection نیز نامیده میشود، هیچ دادهای از یک برنامه وب منتقل نمیشود . به عبارت دقیقتر، مهاجم قادر به دیدن نتیجه حمله از پس از انجام این حمله نیست و تنها به دنبال مشاهده رفتار سرور است . لازم به توضیح است که دو بردار حمله مبتنی بر تزریق کد استنتاجی بهنامهای Blind-Boolean-based SQL injection و Blind-time-based SQL injection وجود دارد که تعریف آنها به شرح زیر است .

تکنیک Boolean Exploitation

تزریق کد Blind SQL یک تکنیک ارسال درخواست به بانک اطلاعاتی است. پاسخ دریافتی از بانک اطلاعاتی

شامل هیچ دادهای نستی، اما مهاجم قادر است واکنش HTTP را مشاهده کند . با ارزیابی پاسخها، یک مهاجم میتواند تشخیص دهد که تزریق موفقیتآمیز بوده یا شکست خورده است، زیرا تنها پاسخ درست یا غلط باز گردانده میشود و قرار نیست هیچ اطلاعاتی از بانکاطلاعاتی دریافت شود .

گروه سوم ، **Out-of-band SQL Injection**

در تکنیک فوق از کانالهای مختلفی برای تزریق کد و جمعآوری پاسخها استفاده میشود . به همین دلیل برای بهکارگیری این تکنیک لازم است یکسری ویژگیهای خاص شبیه به درخواستهای DNS یا HTTP در سرور پایگاه داده فعال باشد، در نتیجه این تکنیک به ندرت استفاده میشود .

متدولوژیهای تزریق کد **SQL**

جمعآوری اطلاعات و تشخیص آسیبپذیری تزریق **SQL**

در مرحله جمعآوری، اطلاعاتی در ارتباط با برنامه وب، سیستمعامل، بانکاطلاعاتی و ساختار مولفهها به دست میآید. اطلاعات استخراج شده ارزیابی میشوند تا آسیبپذیریها پیدا شده و مورد بهرهبرداري قرار گیرند . اطلاعات را میتوان با استفاده از ابزارها و تکنیکهای مختلفی از جمله تزریق کدها به فیلدهای ورودی جمعآوری کرد تا پاسخها و پیامهای خطا مشاهده شوند . ارزیابی فیلد رودی ، فیلدهای پنهان، درخواستهای دریافت و ارسال، کوکیها، مقادیر رشتهای و جزییات پیامهای خطا میتواند اطلاعات کافی را برای حمله اولیه تزریق در اختیار هکر قرار دهد .

در شماره آینده مبحث فوق را ادامه میدهیم .

برای مطالعه رایگان تمام بخشهای دوره **CEH** روی لینک زیر کلیک کنید :

آموزش رایگان دوره CEH

نویسنده :
حمیدرضا تائبی
دسته بندی:
امنیت
تاریخ انتشار :
13:50 - 11/04/1399

برچسب:
دوره CEH - آموزش رایگان CEH - آموزش رایگان دوره CEH - هکر کلاه سفید - آموزش CEH v10 - آموزش رایگان CEH10 - هک اخلاقی - ویروس - حمیدرضا تائبی - تزریق کد SQL

نشانی:
https://www.shabakeh-mag.com/security/17025/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-ceh-%D9%87%DA%A9%D8%B1-%DA%A9%D9%84%D8%A7%D9%87-%D8%B3%D9%81%DB%8C%D8%AF-%D9%87%DA%A9%D8%B1%D9%87%D8%A7-%DA%86%DA%AF%D9%88%D9%86%D9%87-%D8%A8%D9%87-%D8%A8%D8%B1%D9%86%D8%A7%D9%85%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%D9%88%D8%A8%E2%80%8C%D9%85%D8%AD%D9%88%D8%B1-%D8%AD%D9%85%D9%84%D9%87-%D9%85%DB%8C%E2%80%8C%DA%A9%D9%86%D9%86%D8%AF%D8%9F