VAPT REPORT

Tracking Crazyeg

Enumeration Date:

16 Th October, 2024

TABLE Of CONTENTS

➢ DASHBOARD

➢ ALERT DESCRIPTIONS & POC

DASHBOARD

WEBSITE: tracking.crazyegg.com

Document Title: Web Application Vulnerability Assessment Report Date: 16 Th October, 2024
Classification: Confidential

Document Type: Report

Reporter: Sunil Vikas S

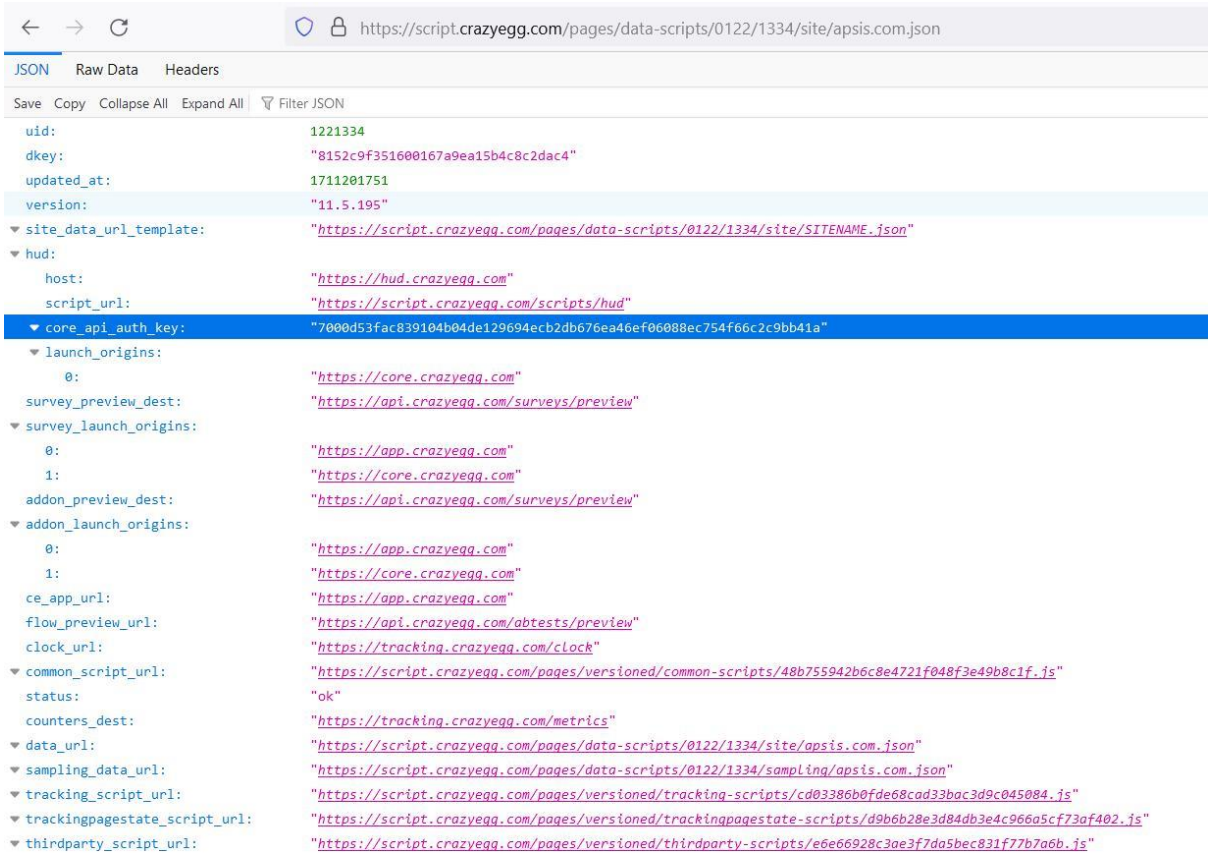
POC:

```
GET /pages/data-scripts/0122/1334/site/apsis.com.json?t=1 HTTP/2
Host: script.crazyegg.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Origin: https://apsis.com
Referer: https://apsis.com/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
If-Modified-Since: Sat, 23 Mar 2024 13:49:11 GMT
Te: trailers


```


```
},
"survey_preview_dest":"https://api.crazyegg.com/surveys/preview",
"survey_launch_origins":[
  "https://app.crazyegg.com",
  "https://core.crazyegg.com"
],
"addon_preview_dest":"https://api.crazyegg.com/surveys/preview",
"addon_launch_origins":[
  "https://app.crazyegg.com",
  "https://core.crazyegg.com"
],
"ce_app_url":"https://app.crazyegg.com",
"flow_preview_url":"https://api.crazyegg.com/abtests/preview",
"clock_url":"https://tracking.crazyegg.com/clock",
"common_script_url":"https://script.crazyegg.com/pages/versioned/common-scripts/48b755942b6c8e4721f048f3e49b8c1f.js",
"status":"ok",
"counters_dest":"https://tracking.crazyegg.com/metrics",
"data_url":"https://script.crazyegg.com/pages/data-scripts/0122/1334/site/apsis.com.json",
"sampling_data_url":"https://script.crazyegg.com/pages/data-scripts/0122/1334/sampling/apsis.com.json",
"tracking_script_url":"https://script.crazyegg.com/pages/versioned/tracking-scripts/cd03386b0fde68cad33bac3d9c045084.js",
"trackingpagestate_script_url":"https://script.crazyegg.com/pages/versioned/trackingpagestate-scripts/d9b6b28e3d84db3e4c966a5cf73af402.js",
"thirdparty_script_url":"https://script.crazyegg.com/pages/versioned/thirdparty-scripts/e6e66928c3ae3f7da5bec831f77b7a6b.js",
"sites":
"%8&4!}%|%|!}$<$5$4$9$2$6$7$,!}&%%?&$%^!}$<!}%?&(&+%|&+$.%[&&&$!}$,!}&+%^&+&+%|&&&%%.%^%[&&&*%]%|&%%`!}$<&,&*&-%^$,!}&*%^%[&&&*%]%|&%%`%0%^&,&,%|&%%`&+!
}$<&4!}&(%?%`%^%1%?&*%`%^&,%|&%%`$|&%%?%@&!%^%]!}$<%_%?&!&+%^$,!}&(%?%`%^%1%?&*%`%^&,%|&%%`%2&*&!&+!}$<%8%;$,!}&*&-&!%^&+!}$<%8%;$,!}&$%?&+%~$|&!%^&$%^&
%&,&+!}$<&%&-&!&!$,!}&+%?&$&(&!%|&%%`%0&,&*%?&,%^%`&2!}$<!}&-&%%|%_&&&*&$!}$,!}&+%?&$&(&!%|&%%`%*&-&$%.%^%[&&&*%]%|&%%`&+!}$<&%&-&!&!$,!}&+%?&$&(&!%|&%
`%0&,%?&*&,${%?&,%^!}$<&%&-&!&!$,!}&+%?&$&(&!%|&%%`%0&,%?&*&,${%?&,%^%26%%|&l!}$<&%&-&!&!$,!}&+%?&$&(&!%|&%%`$|&%%]${%?&,%^!}$<&%&-&!&!$,!}&+%?&$&(&!%|&
%%`$|&%%]${%?&,%^%2&%%|&l!}$<&%&-&!&!$,!}&+%?&$&(&!%|&%%`%2&(%]%?&,%^%]$^&,!}$<&%&-&!&!$,!}%^&%%]%0%^&+&+%|&&&%%+&%$_&!&&%[%~%^%]%2&*&!!}$<%_%?&!&+%^$,!
}%@&!&&%[%~%^%]%2&*&!&+!}$<%8%;$,!}%@&!&&%[%~%^%]%.&-&!%^&+!}$<%8%;$,!}&(&*%^$`%?%[%{%^%$&$%?%`%^&+!}$<%_%?&!&+%^$,!}&*%^%[&&&*%]%$_&*%?&$%^&+!}$<%_%?&
!&+%^$,!}%{%|%]%^%$%_&*%?&$%^&+!}$<%_%?&!&+%^$,!}&+%?&$&(&!%|&%%`$`&&&$&(&!%^&,%^%]$^&,!}$<$2$8$1$;$3$2$6$9$9$9&6$,!}&*%^%[&&&*%]%|&%%`%=&*%?&,%|&&!}$<$
9&6%;",
"global_ip_block_list":
"$2$;$5$.$8$9$.$8$9$.$2$8$5!.$2$8$3$.$3$8$.$3$3$6$.$3$1$5!.$9$3$.$7$5$.$5$6$.$2$5$4!.$3$.$2$1$;$.$6$7$.$2$7$3!.$3$.$2$4$9$.$2$5$9$.$8!.$2$5$7$.$3$5$8$.$
2$8$7$.$2$6$1!.$3$.$2$4$9$.$2$6$;$.$2$3$4!.$;$2$.$2$7$9$.$2$5$.$2$;$9!.$9$2$.$3$3$5$.$4$6$.$2$7$;!.",
"is_using_ip_blocking":true,
```


```
HTTP/2 200 OK
Date: Sun, 24 Mar 2024 13:45:47 GMT
Content-Type: application/json
Content-Length: 5496
Access-Control-Expose-Headers: CE-Version
Ce-Version: 11.5.195
Cache-Control: public, max-age=300, s-maxage=1209600
Timing-Allow-Origin: *
Last-Modified: Sun, 24 Mar 2024 12:49:49 GMT
Access-Control-Allow-Origin: *
Cf-Cache-Status: HIT
Age: 3358
Accept-Ranges: bytes
Vary: Accept-Encoding
Server: cloudflare
Cf-Ray: 86971a87dfb293b5-BBI

{
```


```
  "uid":1221334,
  "dkey":"8152c9f351600167a9ea15b4c8c2dac4",
  "updated_at":1711284589,
  "version":"11.5.195",
  "site_data_url_template":"https://script.crazyegg.com/pages/data-scripts/0122/1334/site/SITENAME.json",
  "hud":{
    "host":"https://hud.crazyegg.com",
    "script_url":"https://script.crazyegg.com/scripts/hud",
    "core_api_auth_key":"7000d53fac839104b04de129694ecb2db676ea46ef06088ec754f66c2c9bb41a",
    "launch_origins":[
      "https://core.crazyegg.com"
    ]
  },
  "survey_preview_dest":"https://api.crazyegg.com/surveys/preview",
  "survey_launch_origins":[
    "https://app.crazyegg.com",
    "https://core.crazyegg.com"
  ],
```



https://script.crazyegg.com/pages/data-scripts/0122/1334/site/apsis.com.json

JSON Raw Data Headers

Save Copy Collapse All Expand All Filter JSON


```
uid: 1221334
dkey: "8152c9f351600167a9ea15b4c8c2dac4"
updated_at: 1711201751
version: "11.5.195"
site_data_url_template: "https://script.crazyegg.com/pages/data-scripts/0122/1334/site/SITENAME.json"
hud:
  host: "https://hud.crazyegg.com"
  script_url: "https://script.crazyegg.com/scripts/hud"
  core_api_auth_key: "7000d53fac839104b04de129694ecb2db676ea46ef06088ec754f66c2c9bb41a"
  launch_origins:
    0: "https://core.crazyegg.com"
survey_preview_dest: "https://api.crazyegg.com/surveys/preview"
survey_launch_origins:
  0: "https://app.crazyegg.com"
  1: "https://core.crazyegg.com"
addon_preview_dest: "https://api.crazyegg.com/surveys/preview"
addon_launch_origins:
  0: "https://app.crazyegg.com"
  1: "https://core.crazyegg.com"
ce_app_url: "https://app.crazyegg.com"
flow_preview_url: "https://api.crazyegg.com/abtests/preview"
clock_url: "https://tracking.crazyegg.com/clock"
common_script_url: "https://script.crazyegg.com/pages/versioned/common-scripts/48b755942b6c8e4721f048f3e49b8c1f.js"
status: "ok"
counters_dest: "https://tracking.crazyegg.com/metrics"
data_url: "https://script.crazyegg.com/pages/data-scripts/0122/1334/site/apsis.com.json"
sampling_data_url: "https://script.crazyegg.com/pages/data-scripts/0122/1334/sampling/apsis.com.json"
tracking_script_url: "https://script.crazyegg.com/pages/versioned/tracking-scripts/cd03386b0fde68cad33bac3d9c045084.js"
trackingpagestate_script_url: "https://script.crazyegg.com/pages/versioned/trackingpagestate-scripts/d9b6b28e3d84db3e4c966a5cf73af402.js"
thirdparty_script_url: "https://script.crazyegg.com/pages/versioned/thirdparty-scripts/e6e66928c3ae3f7da5bec831f77b7a6b.js"
```



```
HTTP/2 200 OK
Server: awselb/2.0
Date: Sun, 24 Mar 2024 13:45:35 GMT
Content-Type: application/json
Content-Length: 3499
Access-Control-Allow-Origin: *

{"url":"https://pagestates-tracking.crazyegg.com","fields":{"Content-Type":"application/json","
Content-Encoding":"gzip","Cache-Control":"max-age=31536000, public","x-amz-meta-parent":
"3833cd081d0e3ac8f09f86eb2a25f1f3","bucket":"ce-pagestates-production",
"X-Amz-Algorithm":"AWS4-HMAC-SHA256","X-Amz-Credential":"ASIASOZPXEOHZB6AFWUI/20240324/us-east-1/s3/aws4_request",
"X-Amz-Date":"20240324T134535Z",
"X-Amz-Security-Token":"IQoJb3JpZ2luX2VjEFQaDmFvLXNvdXRoZWFzdC0xIkcwRQIhAKVjm7y5GfaWgdPL3ElykPJNodnjPPsowrfe62OY4e5bAiA3QpxXeJuDErPMWwQEnq+c9BYkBIBbtEJAXzljiticiSqUAwh2EAAaCDE3MzUwOTM4NzE1MSIMHqhl9+V+UsURqBWeKvECAdjztvf
sxAOEDLfw5Uk9tBFmAcWQcW7R7GaeFaM5Xy+GuYzGenbnCElGlX+zix6g+qe3scDE07XoiA7BrHs6iRoSVils6q4RlBS2hwi3M6ebkxwfWfkA9Xl1JXgsgXDHJ8z+kjOlj9vfOXex8bPs+5CZ6pYY5yxdAAJVkuchAKgYUV3Cm2ez8HWxMKmBkBLl6WJWkcSXu2DykNALioMNG7gLAGOpOBu/
72c7aec62f09fc7a555d.json","Policy":"eyJleHBpcmF0aW9uIjoiMjAyNCOwMyOyNFQxMzo0ODozNVoiLCJjb25kaXRpb25zIjpbeyJDb250ZW50LVR5cGUiOiJhcHBsaWNhdGlvbi9qc29uIn0seyJDb250ZW50LUVuY29kaW5nIjoiZ3ppcCJ9LHsiQ2FjaGUtQ29udHJvbCI6Im1heC
tZWFzdC0xLSMzL2F3czRfcmVxdWVzdCJ9LHsiWC1BbXotRGF0ZSI6IjIwMjQwMzI0VDEzNDUzNVoifSx7ImtGW16LVNlY3VyaXR5LVRva2VuIjoiSVFvSmIzSnBaMmx1WDJWakVGMGFEbUZ3TFhOdmRYUm9aV0Z6ZEMweElrY3dSUUloQUtWam03eTVHZmFXZ2RQTDNFMXlrRkp0b2RualBQc:
MUEEwWlIOcmlYQUNUbDVHcndFdzlMa21Qb1g4eVpxMOtOS2V5ZEFjdEZ4NGg2MEdaYjc0czZaSOU2VnJVSEsyOHAld2JhdEhEbUZuU3cwNDd1OEljWmtOekpVMVpMRko2WnhONjk2MjJLRWRZTE5UR1ByM1NKNGt2N2ptR1dvekdoZnVkblZER2xFRTErNVRTSzZUYzZxTnEvbGNud2FXUkw5K:
XS2NTNHUyPmUrTkPMaW9NTkc3ZOxBR09wME1lLyt6eW1zTEgyTWNFZDUxVGpjRTl3Y1ZGeTVlck0W5mlsL1dVVGpYajRDK1RCK25QK0JyOWwzek1VZDlwY3ZwdWM4MStqZ1pocnRKYkVMNGEraENYRkVwZzFaVHNONOkwRFBwekg3T2xEMG50WGh4UzBFck1qTUtWMjkwNHhjZk5uN2MzdGhYe:
c4e0960be5acd24e0f863e3aa96ef0c20a9abcc6e1a"},"prefix":"apsis.com/6666cd76f96956469e7be39d750cc7d9"}
```



```
POST /v11/page-states?md5=17589298935972c7aec62f09fc7a555d&url=https://apsis.com/&uid=1221334&tk=f0a19ba9580a4a6dcbeele3c93e03084&parent_md5=3833cd081d0e3ac8f09f86eb2a25f1f3 HTTP/1.1
Host: tracking.crazyegg.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Origin: https://apsis.com
Referer: https://apsis.com/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Content-Length: 0
Te: trailers
Connection: close
```