

Forum:[Hack Forums](#)

Thread: [Authentication Bypass - htaccess exploitation](#)

nerdy - May 18, 2022, 9:18 am

htaccess exploitation

? Here i will cover about a misconfiguration which many sysadmins make. ?

[1] BASIC MISCONFIG

It depends on how the htaccess is configured, many sysadmins commit misconfigurations and that leads to shit like this.

Example:

```
Code AuthUserFile /location/.htpasswd
AuthName "Restricted Area."
AuthType Basic
```

```
<Limit GET POST>
```

```
require valid-user
```

```
</Limit>
```

What's wrong here?

Problem comes at here:

```
Code <Limit GET POST>
```

```
require valid-user
```

```
</Limit>
```

It limits only for GET and POST requests. An attacker could use other requests like PUT and bypass it.

For example:

```
Code curl -X PUT targetLinkTo/protected-area
```

weeboi - May 31, 2022, 6:38 am

I think restriction bypass would be a more appropriate term, since this is commonly used to bypass 403 errors.

linkinpork - May 31, 2022, 7:30 am

(May 18, 2022 09:18 AM)nerdy Wrote: [\[CITE\]](#) ? Here i will cover about a misconfiguration which many sysadmins make. ?

This isn't authentication bypass.

Authentication bypass looks like this:

Here's OWASP's guide on Auth Bypass:

https://owasp.org/www-project-top-ten/2017/A2_2017-Broken_Authentication

Exxxotic - June 2, 2022, 3:51 am

(May 31, 2022 06:38 AM)weeboi Wrote: [\[CITE\]](#) I think restriction bypass would be a more appropriate term, since this is commonly used to bypass 403 errors.

did you really just brute force this person that fast?!?

NS25 - July 7, 2022, 2:19 am

Htaccess restriction bypass would be a more appropriate term for this

Brief - November 14, 2022, 6:35 am

How would one find "protected-area" (assuming it's a path or file)? In my knowledge, fuzzing those links requires GET request. Won't the requests to find the protected-area be blocked? Correct me if I am talking about something unrelated here. I don't even know what .htaccess is.