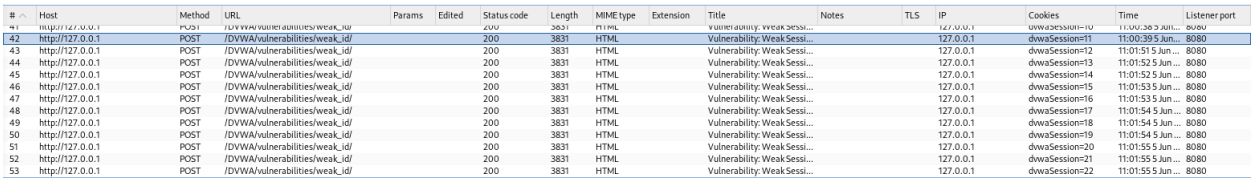
Weak Session IDs

Using burp suite and look at the associated requests in Burp Suite `Proxy > HTTP history`

1. **Low level**



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
42	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/			200	3831	HTML		Vulnerability: Weak Sessi...			127.0.0.1	dvwaSession=11	11:00:39 5 Jun ...	8080
43	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/			200	3831	HTML		Vulnerability: Weak Sessi...			127.0.0.1	dvwaSession=12	11:01:51 5 Jun ...	8080
44	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/			200	3831	HTML		Vulnerability: Weak Sessi...			127.0.0.1	dvwaSession=13	11:01:52 5 Jun ...	8080
45	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/			200	3831	HTML		Vulnerability: Weak Sessi...			127.0.0.1	dvwaSession=14	11:01:52 5 Jun ...	8080
46	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/			200	3831	HTML		Vulnerability: Weak Sessi...			127.0.0.1	dvwaSession=15	11:01:53 5 Jun ...	8080
47	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/			200	3831	HTML		Vulnerability: Weak Sessi...			127.0.0.1	dvwaSession=16	11:01:53 5 Jun ...	8080
48	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/			200	3831	HTML		Vulnerability: Weak Sessi...			127.0.0.1	dvwaSession=17	11:01:54 5 Jun ...	8080
49	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/			200	3831	HTML		Vulnerability: Weak Sessi...			127.0.0.1	dvwaSession=18	11:01:54 5 Jun ...	8080
50	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/			200	3831	HTML		Vulnerability: Weak Sessi...			127.0.0.1	dvwaSession=19	11:01:54 5 Jun ...	8080
51	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/			200	3831	HTML		Vulnerability: Weak Sessi...			127.0.0.1	dvwaSession=20	11:01:55 5 Jun ...	8080
52	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/			200	3831	HTML		Vulnerability: Weak Sessi...			127.0.0.1	dvwaSession=21	11:01:55 5 Jun ...	8080
53	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/			200	3831	HTML		Vulnerability: Weak Sessi...			127.0.0.1	dvwaSession=22	11:01:55 5 Jun ...	8080

- The value of the cookie in incremented by one everytime we click on the button **Generate**
- With these cookies we can steal a valid user session and impersonate a legitimate user to steal information or carry out some malicious operations
- Review code

```
<?php$html = "";

if ($_SERVER['REQUEST_METHOD'] == "POST") {
    if (!isset ($_SESSION['last_session_id'])) {
        $_SESSION['last_session_id'] = 0;
    }
    $_SESSION['last_session_id']++;
    $cookie_value = $_SESSION['last_session_id'];
    setcookie("dvwaSession", $cookie_value);
}
?>
```

- The code on the server simply adds one to the previous session id `$_SESSION['last_session_id']++;`
- To prevent this kind of vulnerability, the session ID should be hard to find for an attacker

2. **Medium level**

59	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/	200	3848	HTML	Vulnerability: Weak Sessi...	127.0.0.1	dvwaSession=1717600018	11:06:58 5 Jun ...	8080
60	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/	200	3848	HTML	Vulnerability: Weak Sessi...	127.0.0.1	dvwaSession=1717600019	11:06:59 5 Jun ...	8080
61	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/	200	3848	HTML	Vulnerability: Weak Sessi...	127.0.0.1	dvwaSession=1717600019	11:06:59 5 Jun ...	8080
62	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/	200	3848	HTML	Vulnerability: Weak Sessi...	127.0.0.1	dvwaSession=1717600019	11:06:59 5 Jun ...	8080
63	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/	200	3848	HTML	Vulnerability: Weak Sessi...	127.0.0.1	dvwaSession=1717600019	11:06:59 5 Jun ...	8080
64	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/	200	3848	HTML	Vulnerability: Weak Sessi...	127.0.0.1	dvwaSession=1717600020	11:07:00 5 Jun ...	8080
65	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/	200	3848	HTML	Vulnerability: Weak Sessi...	127.0.0.1	dvwaSession=1717600020	11:07:00 5 Jun ...	8080
66	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/	200	3848	HTML	Vulnerability: Weak Sessi...	127.0.0.1	dvwaSession=1717600020	11:07:00 5 Jun ...	8080
67	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/	200	3848	HTML	Vulnerability: Weak Sessi...	127.0.0.1	dvwaSession=1717600020	11:07:00 5 Jun ...	8080
68	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/	200	3848	HTML	Vulnerability: Weak Sessi...	127.0.0.1	dvwaSession=1717600021	11:07:01 5 Jun ...	8080

- The cookie is different and might be impredictible
- When we glance at some of the cookies values, we can see that they all look like
    - 1717807718
    - 1717807719
    - 1717807720
    - 1717807721
- It seeem the values are increasing.
- Review code

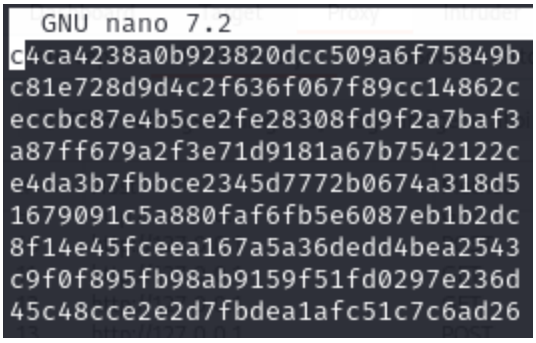
```
<?php$html = "";

if ($_SERVER['REQUEST_METHOD'] == "POST") {
    $cookie_value = time();
    setcookie("dvwaSession", $cookie_value);
}
?>
```

- The code just calls `time()` to set the cookie value
- The cookies should be hard to find. The attacker should not be able to perform a statistical analysis on a dataset to understand how they are generated

3. **High level**

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies
10	http://127.0.0.1	POST	/DVWA/security.php	✓		302	568	HTML	php				127.0.0.1	security=high; PHPSESSID=jdjv0iqo78q9d8pndjkhf10mvj; PHP...
11	http://127.0.0.1	GET	/DVWA/security.php			200	4942	HTML	php	DVWA Security :: Damn V...			127.0.0.1	
12	http://127.0.0.1	GET	/DVWA/vulnerabilities/weak_id/			200	3806	HTML		Vulnerability: Weak Sessi...			127.0.0.1	
13	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/			200	3967	HTML		Vulnerability: Weak Sessi...			127.0.0.1	dvwaSession=c4ca4238a0b923820dcc509a6f75849b
14	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/			200	3967	HTML		Vulnerability: Weak Sessi...			127.0.0.1	dvwaSession=c81e728d9d4c2f636f067f89cc14862c
15	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/			200	3967	HTML		Vulnerability: Weak Sessi...			127.0.0.1	dvwaSession=eccbc87e4b5ce2fe28308fd9f2a7baf3
16	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/			200	3967	HTML		Vulnerability: Weak Sessi...			127.0.0.1	dvwaSession=a87ff679a2f3e71d9181a67b7542122c
17	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/			200	3967	HTML		Vulnerability: Weak Sessi...			127.0.0.1	dvwaSession=e4da3b7fbbce2345d7772b0674a318d5
18	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/			200	3967	HTML		Vulnerability: Weak Sessi...			127.0.0.1	dvwaSession=1679091c5a880faf6fb5e6087eb1b2dc
19	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/			200	3967	HTML		Vulnerability: Weak Sessi...			127.0.0.1	dvwaSession=8f14e45fceea167a5a36dedd4bea2543
20	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/			200	3967	HTML		Vulnerability: Weak Sessi...			127.0.0.1	dvwaSession=c9f0f895fb98ab9159f51fd0297e236d
21	http://127.0.0.1	POST	/DVWA/vulnerabilities/weak_id/			200	3967	HTML		Vulnerability: Weak Sessi...			127.0.0.1	dvwaSession=45c48cce2e2d7fbdea1afc51c7c6ad26

- The cookies were hashes. It look like MD5 hashs



- Crack these hashes with hashcat

- Review code

```
<?php$html = "";

if ($_SERVER['REQUEST_METHOD'] == "POST") {
    if (!isset ($_SESSION['last_session_id_high'])) {
        $_SESSION['last_session_id_high'] = 0;
    }
    $_SESSION['last_session_id_high']++;
    $cookie_value = md5($_SESSION['last_session_id_high']);
    setcookie("dvwaSession", $cookie_value, time()+3600, "/vu
```

```
lnerabilities/weak_id/", $_SERVER['HTTP_HOST'], false, fals
e);
}

?>
```

- The cookie value is `md5($_SESSION['last_session_id_high']);`