**REVERSE ENGINEERING PROCESS**

**Thien Tran**

**5xG7GvEvdQnkoKAFUrs1jkrDA42**

Table of Contents

[SELECT\_VULN.PHP 2](#_Toc207912317)

[UPDATE\_VULN.PHP 3](#_Toc207912318)

[INSERT\_VULN.PHP 4](#_Toc207912319)

[DELETE\_VULN.PHP 5](#_Toc207912320)

|  |
| --- |
| SELECT\_VULN.PHP |

1. Normal Behaviour



* Output: User: admin

1. Boolean-Based Blind SQLi



* Output: User: admin



* No results

This confirms injection is possible via conditional logic

1. Time-Based Blind SQLi



* The page slows significantly, confirming the injection working

1. Content-Based Blind SQLi

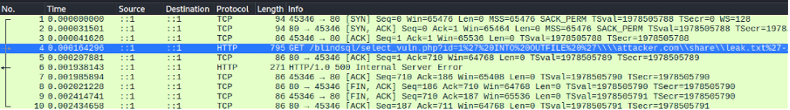
* Output: User: admin. Confirms that there are columns “users” and “password” in the DB

1. Out-of-Band Blind SQLi





* Triggers an outbound DNS/HTTP lookup

****

|  |
| --- |
| UPDATE\_VULN.PHP |

1. Normal Behaviour





* Updates user id=1 password to abc

1. Boolean-Based Blind SQLi





* Updated (query executes)





* Not updated

This proves logical conditions can be injected and inferred

1. Time-Based Blind SQLi





* Response delayed by 5s and password was not updated (confirms injection).

Can be extended to extract schema data by asking yes/no questions:





* Response delayed by 5s and password was not updated (confirm the database name length is 8).

Also, can extract DB name character-by character:



Count tables:



1. Content-Based Blind SQLi



* Updates password (confirms that there are 3 users in the DB)

1. Out-of-Band Blind SQLi





* Triggers an outbound DNS/HTTP lookupA screenshot of a computer

  AI-generated content may be incorrect.

|  |
| --- |
| INSERT\_VULN.PHP |

1. Boolean-Based Blind SQLi



* Row inserted.



* No row inserted

Confirms Boolean-based blind SQLi works.

1. Time-Based Blind SQLi



* Page delayed 5s then row inserted

1. Content-Based Blind SQLi



* Inserted as users table has more than 2 rows

1. Out-of-Band Blind SQLi



* Didn’t inserted but triggered an outbound DNS/HTTP lookup **A screenshot of a computer

  AI-generated content may be incorrect.**

|  |
| --- |
| DELETE\_VULN.PHP |

1. Normal Behaviour
2. Boolean-Based Blind SQLi



* Deleted all rows



* Deleted nothing

1. Time-Based Blind SQLi



* Only delayed, didn’t delete.

1. Content-Based Blind SQLi

* Only delete specify user id

1. Out-of-Band Blind SQLi

* Attempts outbound DNS/HTTP

